Content Security Gateway

CS-500

User's Manual

Copyright

Disclaimer

PLANET Technology does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose.
PLANET has made every effort to ensure that this User's Manual is accurate; PLANET disclaims liability for any inaccuracies or omissions that may have occurred.
Information in this User's Manual is subject to change without notice and does not represent a commitment on the part of PLANET. PLANET assumes no responsibility for any inaccuracies that may be contained in this User's Manual. PLANET makes no commitment to update or keep current the information in this User's Manual, and reserves the right to make improvements to this User's Manual and/or to the products described in this User's Manual, at any time without notice.
If you find information in this manual that is incorrect, misleading, or incomplete, we would appreciate your comments and suggestions.

CE mark Warning

This is a class B device, in a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Trademarks

The PLANET logo is a trademark of PLANET Technology.
This documentation may refer to numerous hardware and software products by their trade names. In most, if not all cases, these designations are claimed as trademarks or registered trademarks by their respective companies.

Customer Service

For information on customer service and support for the Content Security Gateway, please refer to the following Website URL:

http://www.planet.com.tw

Before contacting customer service, please take a moment to gather the following information:

- Content Security Gateway serial number and MAC address
- Any error messages that displayed when the problem occurred
- Any software running when the problem occurred
- Steps you took to resolve the problem on your own

Revision

User's Manual for PLANET Content Security Gateway

Model: CS-500

Rev: 3.0 (May, 2006)

Part No. EM-CS500v3

Table of Contents

Chapter 1: Introduction

The innovation of the Internet has created a tremendous worldwide venue for e-business and information sharing, but it also creates network security problems, so the security request will be the primary concerned for the enterprise. Planet's Content Security Gateway CS-500, a special designed of security gateway for small business, adopts Heuristics Analysis to filter spam and virus mail, auto-training system can raise identify rate of spam, and built-in Clam virus scan engine can detect viruses, worms and other threats from email transfer.

Meanwhile, Instant Messaging (IM) and peer-to-peer (P2P) are the fastest growing communications medium of all time, the spread of IM and P2P has created a network security threats and consumed amount of bandwidth. CS-500 also can prevent employees using varied IM and P2P like MSN, Yahoo Messenger, ICQ, QQ and Skype.

CS-500 not only can filter spam and virus mail, but also is a high performance VPN firewall. The IDP and firewall function can defense hacker and blaster attack from Internet. Moreover, built-in QoS feature can let you configure the traffic per specific protocol more flexibly. The completely function in one device can offers an excellent security solution and the secure environment for the SMB or SOHO users.

1.1 Features

- **Anti-Spam Filtering:** Multiple defense layers (Head Analysis, Text Analysis, Blacklist & Whitelist, Bayesian Filtering), and Heuristics Analysis to block over 95% spam mail. Customizable notification options and spam mail report are provided for administrator. Varied actions toward spam mail include: Delete, Deliver, and Forward. Built-in auto-training system to rise identify rate of spam mail substantially.

- **Anti-Virus Protection:** Built-in Clam virus scan engine can detect viruses, worms, and other threats from email transfer. Scan mission-critical content protocols-SMTP, POP in real time as traffic enters the network to provide maximum protection. Customizable notification options and virus mail report are provided for administrator. Varied actions toward spam mail include: Delete, Deliver, and Forward.

- **Policy-based Firewall:** The built-in policy-based firewall prevent many known hacker attack including SYN attack, ICMP flood, UDP flood, Ping of Death, etc. The access control function allowed only specified WAN or LAN users to use only allowed network services on specified time.

- **VPN Connectivity:** The security gateway support PPTP server/client and IPSec VPN. With DES, 3DES and AES encryption and SHA-1 / MD5 authentication, the network traffic over public Internet is secured.

- **Content Filtering:** The security gateway can block network connection based on URLs, Scripts (The Pop-up, Java Applet, cookies and Active X), P2P (eDonkey, Bit Torrent, WinMX and Foxy), Instant Messaging (MSN, Yahoo Messenger, ICQ, QQ and Skype), Download and Upload.

- **IDP:** CS-500 provides three kinds of the Signature to complete the intrusion detection system, user can select to configure "**Anomaly**", "**Pre-defined**" and "**Custom**" according to the current environment's request.

- **QoS:** You can control the outbound and inbound Upstream/downstream Bandwidth by configuring the QoS based on the WAN bandwidth.

- **User Authentication:** Web-based authentication allows users to be authenticated by web browser. User database can be configured on the devices or through external RADIUS server.

- **Multiple NAT:** Multiple NAT allows local port to set multiple subnet works and connect to the Internet through different WAN IP addresses.

1.2 Package Contents

The following items should be included:

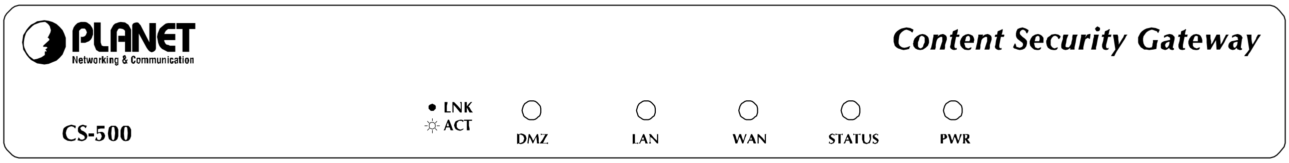
CS-500

- ■ Content Security Gateway
- ■ User's Manual CD-ROM
- ■ This Quick Installation Guide
- ■ Power Adapter

If any of the contents are missing or damaged, please contact your dealer or distributor immediately.

1.3 Content Security Gateway Front View

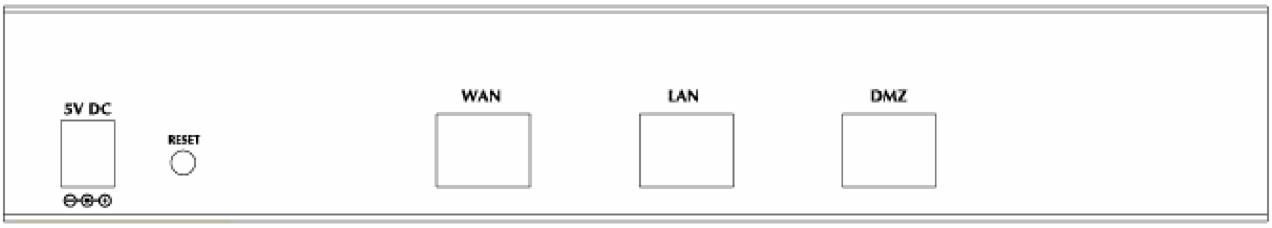
CS-500 Front Panel



LED	Description
PWR	Power is supplied to this device.
STATUS	Blinks to indicate this devise is being turned on and booting. After one minute, this LED indicator will stop blinking, it means this device is now ready to use.
WAN, LAN, DMZ	Steady on indicates the port is connected to other network device. Blink to indicates there is traffic on the port

1.4 Content Security Gateway Rear Panel

CS-500 Rear Panel



Port or button	Description
RESET	Press this button to restore to factory default

	settings.
WAN	Connect to your xDSL/Cable modem or other Internet connection devices
LAN	Connect to your local PC, switch or other local network device
DMZ	Connect to your server or other network device

1.5 Specification

Product		Content Security Gateway
Model		CS-500
Hardware		
Ethernet	LAN	1 x 10/100Mbps RJ-45
	WAN	1 x 10/100Mbps RJ-45
	DMZ	1 x 10/100Mbps RJ-45
LED		POWER, STATUS, 10/100 and LNK/ACT for each LAN and WAN port
Power		5VDC, 2.4A
Operating Environment		Temperature: 0~50°C Relative Humidity: 10%~90%
Dimension W x D x H, mm		220 x 150 x 40
Regulatory		FCC, CE Mark
Software		
Management		Web
Network Connection		Transparent mode (WAN to DMZ), NAT, Multi-NAT
Routing Mode		Static Route, RIPv2
Concurrent Sessions		110,000
New session / second		8,000
Email Capacity per Day		90,000
Firewall Throughout		100Mbps
3DES Throughput		15Mbps
Firewall		Policy-based firewall rule with schedule, NAT/NAPT, SPI firewall
VPN Tunnels		200
VPN Function		PPTP server and client, IPSec DES, 3DES and AES encryption, SHA-1 and MD5 authentication algorithm Remote access VPN (client-to-Site) and Site to Site VPN
Content Filtering		URL, P2P application, Instant Message, download & upload blocking Popup, Java Applet, cookies and Active X blocking
Anomaly Flow IP		Hacker Alert: Sasser, Code Red, Syn Flood, ICMP Flood, UDP Flood, Blaster Alert
Scanning Mail Settings		The allowed size of scanned mail: 10 ~ 512Kbytes
Anti-Virus		Email attachment virus scanning by SMTP, POP3 Inbound scanning for internal and external Mail server Action of infected mail: Delete, Deliver to the recipient, forward to a specific account Automatic or manual update virus database
Anti-Spam		Inbound scanning for external and internal Mail Server Check sender address in RBL Black list and white list support auto training system Action of spam mail: Delete, Deliver to the recipient, forward to a specific account

IDP	Anomaly: Syn Flood, UDP Flood, ICMP Flood and more. Pre-defined : Backdoor, DDoS, DoS, Exploit, NetBIOS and Spyware. Custom: User defined based on TCP, UDP, ICMP or IP protocol.
QoS	Policy rules with Inbound/Outbound traffic management Guaranteed and maximum bandwidth Scheduled in unit of 30 minutes 3 Priorities
User Authentication	Built-in user database with up to 500 entries Support local database, RADIUS and POP3 authentication
Logs	Log and alarm for event and traffic Log can be saved from web, sent by e-mail or send to syslog server
Statistics	Traffic statistics for WAN interface and policies Graphic display
Others	Dynamic DNS, NTP support, DHCP server, Virtual server, Mapping IP (DMZ)

Chapter 2: Hardware Installation

2.1 Installation Requirements

Before installing the Content Security Gateway, make sure your network meets the following requirements.

- Mechanical Requirements

The Content Security Gateway is to be installed between your Internet connection and local area network. The Content Security Gateway can be placed on the table or rack. Locate the unit near the power outlet.

- Electrical Requirements

The Content Security Gateway is a power-required device, it means, the Content Security Gateway will not work until it is powered. If your networked PCs will need to transmit data all the time, please consider use an UPS (Uninterrupted Power Supply) for your Content Security Gateway. It will prevent you from network data loss. In some area, installing a surge suppression device may also help to protect your Content Security Gateway from being damaged by unregulated surge or current to the Content Security Gateway.

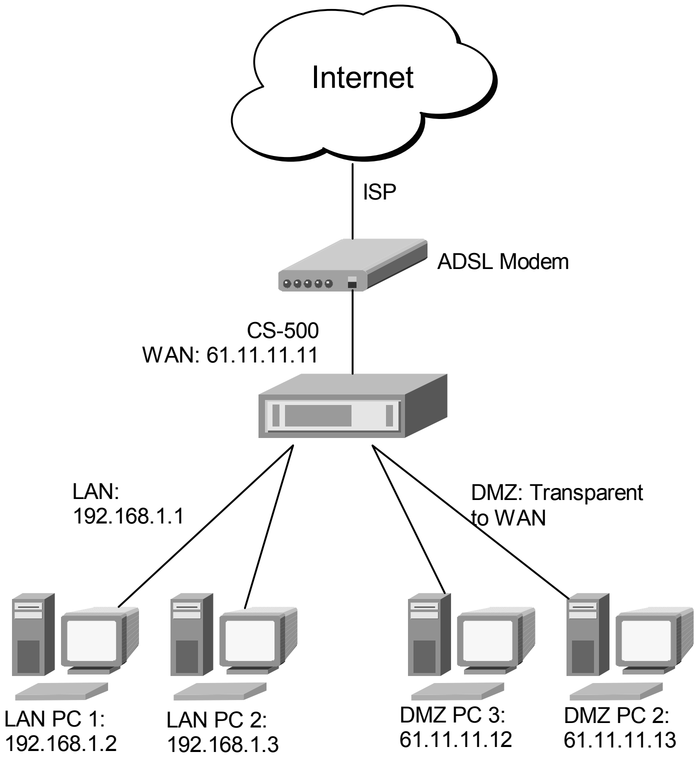
- Network Requirements

In order for Content Security Gateway to secure your network traffic, the traffic must pass through Content Security Gateway at a useful point in a network. In most situations, the Content Security Gateway should be placed behind the Internet connection device.

2.2 Operation Mode

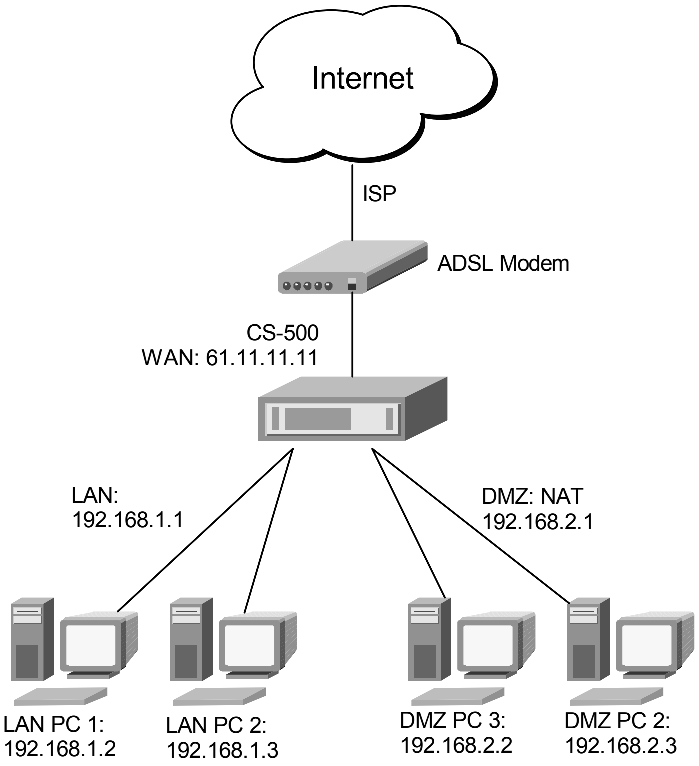
CS-500 DMZ port supports three operation modes, Disable, NAT and Transparent. In Disable mode, the DMZ port is not active. In transparent mode, CS-500 works as proxy with forward DMZ packet to WAN and forward WAN packet to DMZ, the DMZ and WAN side IP addresses are in the same subnet. In NAT mode, DMZ side user will share one public IP address of WAN port to make Internet connection. Please find the following two pictures for example.

2.2.1 Transparent Mode Connection Example



The WAN and DMZ side IP addresses are on the same subnet. This application is suitable if you have a subnet of IP addresses and you do not want to change any IP configuration on the subnet.

2.2.2 NAT Mode Connecting Example



DMZ and WAN IP addresses are on the different subnet. This provides higher security level then transparent mode.

Chapter 3: Getting Started

3.1 Web Configuration

STEP 1:

Connect both the Administrator's PC and the LAN port of the Content Security Gateway to a hub or switch. Make sure there is a link light on the hub/switch for both connections. The Content Security Gateway has an embedded web server used for management and configuration. Use a web browser to display the configurations of the Content Security Gateway (such as Internet Explorer 4(or above) or Netscape 4.0(or above) with full java script support). The default IP address of the Content Security Gateway is **192.168.1.1** with a subnet mask of 255.255.255.0. Therefore, the IP address of the Administrator PC must be in the range between 192.168.1.2– 192.168.1.254

If the company's LAN IP Address is not subnet of 192.168.1.0, (i.e. LAN IP Address is 172.16.0.1), then the Administrator must change his/her PC IP address to be within the same range of the LAN subnet (i.e. 172.16.0.2). Reboot the PC if necessary.

By default, the Content Security Gateway is shipped with its DHCP Server function enabled. This means the client computers on the LAN network including the Administrator PC can set their TCP/IP settings to automatically obtain an IP address from the Content Security Gateway.

The following table is a list of private IP addresses. These addresses may not be used as a WAN IP address.

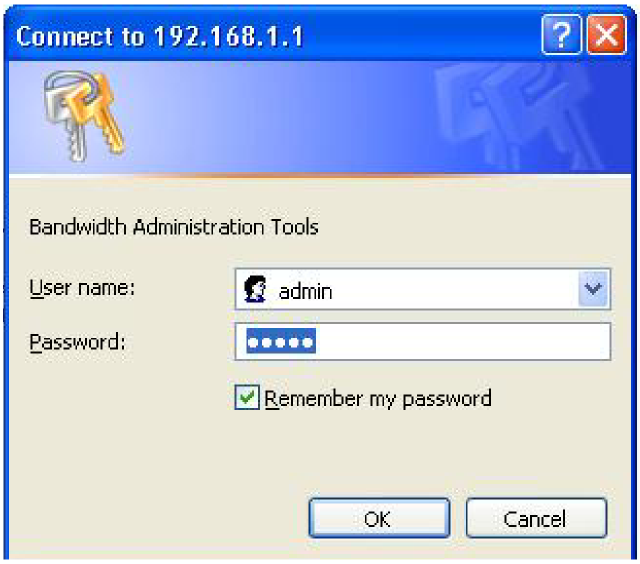
10.0.0.0 ~ 10.255.255.255
172.16.0.0 ~ 172.31.255.255
192.168.0.0 ~ 192.168.255.255

STEP 2:

Once the Administrator PC has an IP address on the same network as the Content Security Gateway, open up an Internet web browser and type in http://192.168.1.1 in the address bar.

A pop-up screen will appear and prompt for a username and password. A username and password is required to connect to the Content Security Gateway. Enter the default login username and password of Administrator (see below).

Username: admin
Password: admin
Click OK.



Connect to 192.168.1.1

Bandwidth Administration Tools

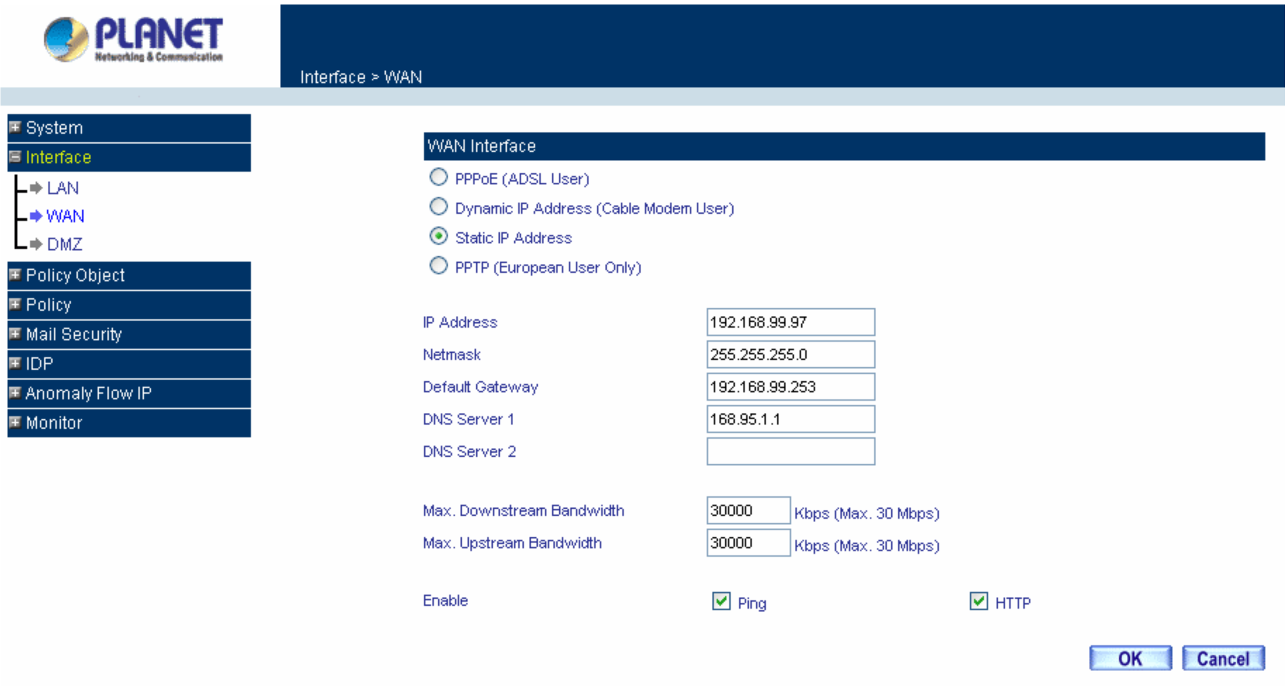
User name: admin

Password: •••••

☑ Remember my password

3.2 Configure WAN interface

After entering the username and password, the Content Security Gateway WEB UI screen will display. Select the **Interface** tab on the left menu then click on WAN below it.
Click on Modify button of WAN, the following page is shown.



WAN Interface

○ PPPoE (ADSL User)
○ Dynamic IP Address (Cable Modem User)
● Static IP Address
○ PPTP (European User Only)

IP Address	192.168.99.97
Netmask	255.255.255.0
Default Gateway	192.168.99.253
DNS Server 1	168.95.1.1
DNS Server 2	
Max. Downstream Bandwidth	30000 Kbps (Max. 30 Mbps)
Max. Upstream Bandwidth	30000 Kbps (Max. 30 Mbps)
Enable	☑ Ping ☑ HTTP

<u>PPPoE (ADSL User):</u> This option is for PPPoE users who are required to enter a username and password in order to connect.

Username: Enter the PPPoE username provided by the ISP.
Password: Enter the PPPoE password provided by the ISP.
IP Address provided by ISP:
Dynamic: Select this if the IP address is automatically assigned by the ISP.
Fixed: Select this if you were given a static IP address. Enter the IP address that is given to you by your ISP.
Service-On-Demand:
The PPPoE connection will automatically disconnect after a length of idle time (no activities). Enter in the amount of idle minutes before disconnection. Enter '0' if you do not want the PPPoE connection to disconnect at all.

<u>For Dynamic IP Address (Cable Modem User):</u> This option is for users who are automatically assigned an IP address by their ISP, such as cable modem users. The following fields apply:

MAC Address: This is the MAC Address of the device. Some ISPs require specified MAC address. If the required MAC address is your PC's, click **Clone MAC Address**.
Hostname: This will be the name assign to the device. Some cable modem ISP assign a specific hostname in order to connect to their network. Please enter the hostname here. If not required by your ISP, you do not have to enter a hostname.
Domain Name: You can specify your own domain name or leave it blank.
User Name: The user name is provided by ISP.
Password: The password is provided by ISP.

<u>For Static IP Address:</u> This option is for users who are assigned a static IP Address from their ISP. Your ISP will provide all the information needed for this section such as IP Address, Netmask, Gateway, and DNS. Use this option also if you have more than one public IP Address assigned to you.

IP Address: Enter the static IP address assigned to you by your ISP. This will be the public IP address of the WAN port of the device.
Netmask: This will be the Netmask of the WAN network. (i.e. 255.255.255.0)

Default Gateway: This will be the Gateway IP address.
Domain Name Server (DNS): This is the IP Address of the DNS server.

For PPTP (European User Only): This is mainly used in Europe. You need to know the PPTP Server address as well as your name and password.

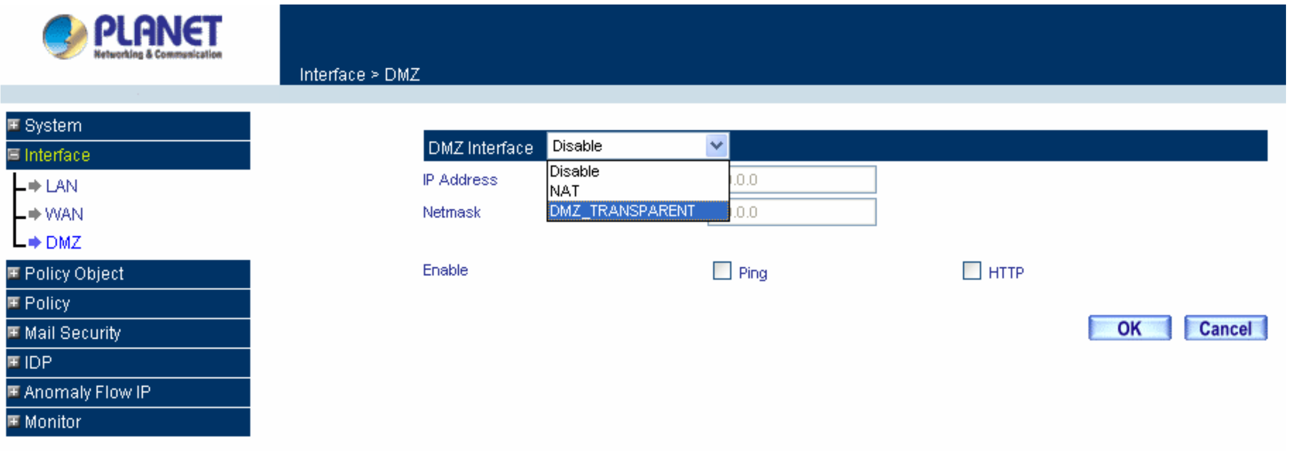
User Name: The user name is provided by ISP.
Password: The password is provided by ISP.
IP Address: Enter the static IP address assigned to you by your ISP, or obtain an IP address automatically from ISP.
PPTP Gateway: Enter the PPTP server IP address assigned to you by your ISP.
Connect ID: This is the ID given by ISP. This is optional.
BEZEQ-ISRAEL: Select this item if you are using the service provided by BEZEQ in Israel.
Service-On-Demand: The PPPoE connection will automatically disconnect after a length of idle time (no activities). Enter in the amount of idle minutes before disconnection. Enter '0' if you do not want the PPPoE connection to disconnect at all.

Ping: Select this to allow the WAN network to ping the IP Address of the Content Security Gateway. This will allow people from the Internet to be able to ping the Content Security Gateway. If set to enable, the device will respond to echo request packets from the WAN network.

WebUI: Select this to allow the device WEBUI to be accessed from the WAN network. This will allow the WebUI to be configured from a user on the Internet. Keep in mind that the device always requires a username and password to enter the WebUI.

3.3 Configure DMZ interface

Depends on your network requirement, you can disable the DMZ port, make DMZ port transparent to WAN or enable NAT function on it.
To configure the DMZ port, select the **Interface** tab on the left menu, then click on DMZ, the following page is shown.



DMZ Interface: Disable
Disable
NAT
DMZ_TRANSPARENT
IP Address .0.0
Netmask .0.0
Enable □ Ping □ HTTP

3.4 Configure Policy

STEP 1:

Click on the **Policy** tab from the main function menu, and then click on **Outgoing** (LAN to WAN) from the sub-function list.

STEP 2:

Click on **New Entry** button.

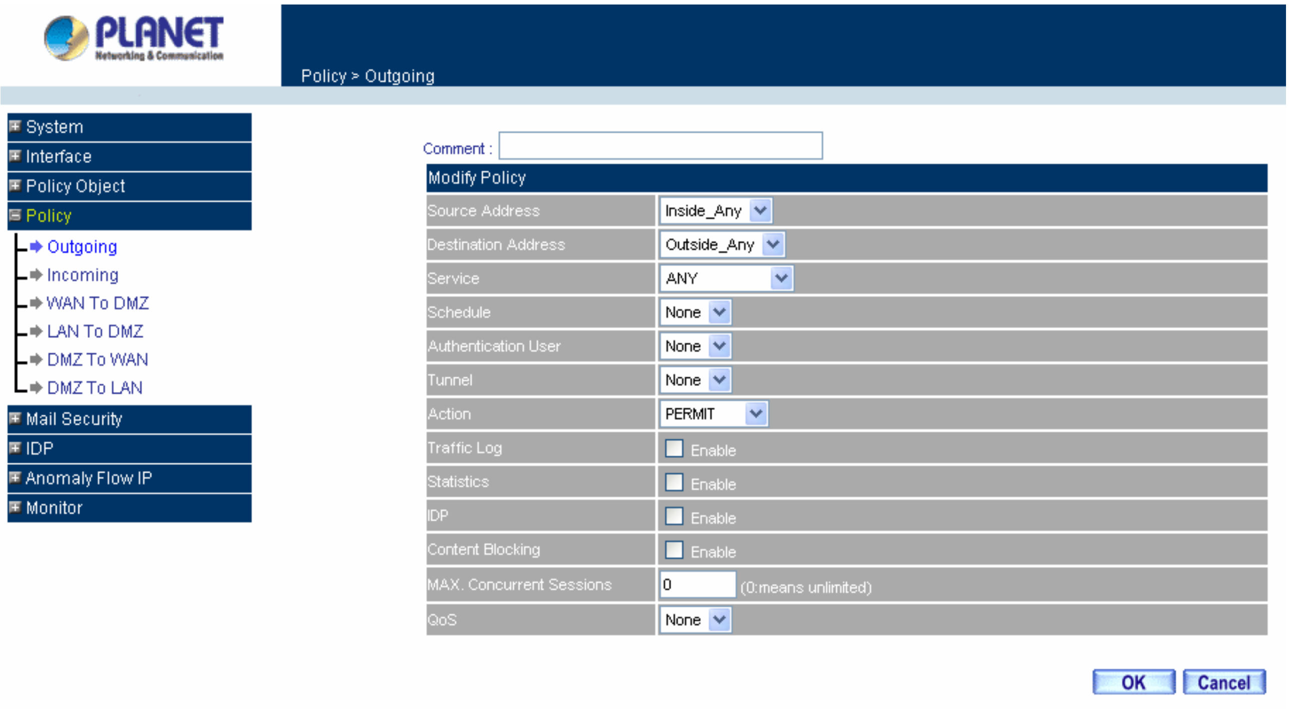
STEP 3:

When the **New Entry** option appears, enter the following configuration:

Source Address – select **"Inside_Any"**

Destination Address – select **"Outside_Any"**
Service - select **"ANY"**
Action - select **"Permit"**

Click on **OK** to apply the changes.

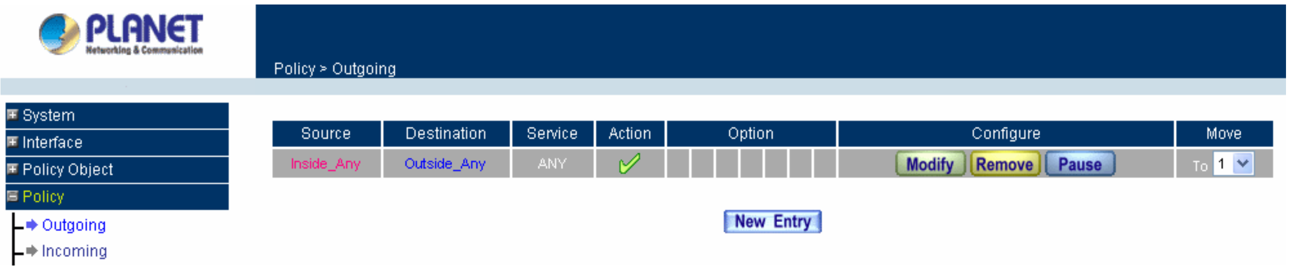


Comment :

Modify Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
Tunnel	None
Action	PERMIT
Traffic Log	□ Enable
Statistics	□ Enable
IDP	□ Enable
Content Blocking	□ Enable
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None

STEP 4:

The configuration is successful when the screen below is displayed.



Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	✓		Modify Remove Pause	To 1

Please make sure that all the computers that are connected to the LAN port have their Default Gateway IP Address set to the Content Security Gateway's LAN IP Address (i.e. 192.168.1.1). At this point, all the computers on the LAN network should gain access to the Internet immediately. If a Content Security Gateway filter function is required, please refer to the Policy section in chapter 4.

Chapter 4: Web Configuration

4.1 System

The Content Security Gateway Administration and monitoring configuration is set by the System Administrator. The System Administrator can add or modify System settings and monitoring mode. The sub Administrators can only read System settings but not modify them. In **System**, the System Administrator can:

1. Add and change the sub Administrator's names and passwords;
2. Back up all Content Security Gateway settings into local files;

"System" is the managing of settings such as the privileges of packets that pass through the Content Security Gateway and monitoring controls. Administrators may manage, monitor, and configure Content Security Gateway settings. All configurations are "read-only" for all users other than the Administrator; those users are not able to change any settings for the Content Security Gateway.

System setting can divide into two parts: **Administration**, **Configure** and **Logout**.

Administration:

Admin: has control of user access to the Content Security Gateway. He/she can add/remove users and change passwords.

Permitted IPs: Enables the Administrator to authorize specific internal/external IP address(es) for Managing Gateway.

Software Update: The administrator can update the device's software with the latest version. Administrators may visit distributor's web site to download the latest firmware. Administrators may update the device firmware to optimize its performance and keep up with the latest fixes for intruding attacks.

Configure:

Setting: The Administrator may use this function to backup Content Security Gateway configurations and export (save) them to an **"Administrator"** computer or anywhere on the network; or restore a configuration file to the device; or restore the Content Security Gateway back to default factory settings. Under **Setting**, the Administrator may enable e-mail alert notification. This will alert Administrator(s) automatically whenever the Content Security Gateway has experienced unauthorized access or a network hit (hacking or flooding). Once enabled, an IP address of a SMTP (Simple Mail Transfer protocol) Server is required. Up to two e-mail addresses can be entered for the alert notifications.

Date/Time: This function enables the Content Security Gateway to be synchronized either with an Internet Server time or with the client computer's clock.

Multiple Subnet: This function allows local port to set multiple subnet works and connect with the internet through WAN IP Addresses.

Route Table: Use this function to enable the Administrator to add static routes for the networks when the dynamic route is not efficient enough.

DHCP: Administrator can configure DHCP (Dynamic Host Configuration Protocol) settings for the LAN (LAN) network.

Dynamic DNS: The Dynamic DNS (require Dynamic DNS Service) allows you to alias a dynamic IP address to a static hostname, allowing your device to be more easily accessed by specific name. When this function is enabled, the IP address in Dynamic DNS Server will be automatically updated with the new IP address provided by ISP.

Host Table: The Content Security Gateway Administrator may use the Host Table function to make the Content Security Gateway act as a DNS Server for the LAN and DMZ network. All DNS requests to a specific Domain Name will be routed to the Content Security Gateway's IP address. For example, let's say an organization has their mail server (i.e., mail.planet.com.tw) in the DMZ network (i.e. 192.168.10.10). The outside Internet world may access the mail server of the organization easily by its domain name, providing that the Administrator has set up Virtual Server or Mapped IP settings correctly. However, for the users in the LAN network, their WAN DNS server will assign them a public IP address for the mail server. So for the LAN network to access the mail server (mail.planet.com.tw), they would have to go out to the Internet, then come back through the Content Security Gateway to access the mail server. Essentially, the LAN network is accessing the mail server by a real public IP address, while the mail server serves their request by a NAT address and not a real one. This odd situation occurs when there are servers in the DMZ network and they are bound to real IP addresses. To avoid this, set up Host Table so all the LAN network computers will use the Content Security Gateway as a DNS server, which acts as the DNS Proxy.

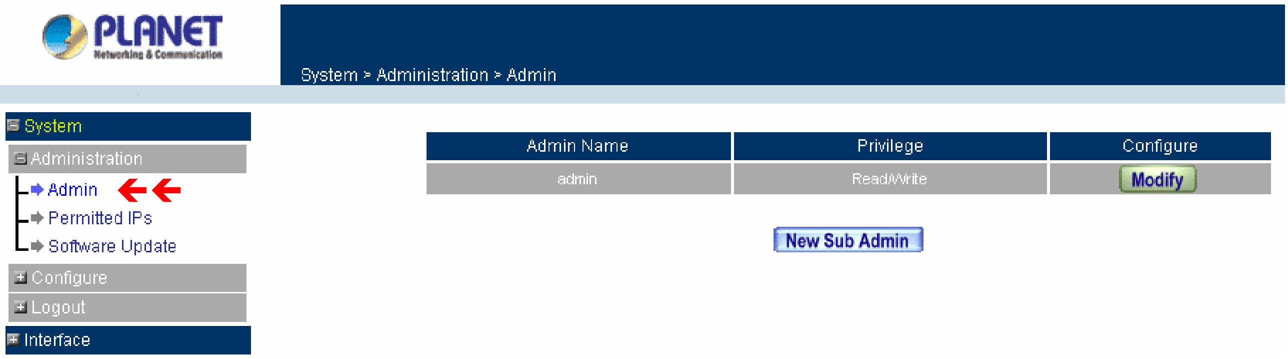
Language: Both Chinese and English are supported in the Content Security Gateway.

Logout:

Logout: Administrator logs out the Content Security Gateway. This function protects your system while you are away.

4.1.1 Admin

On the left hand menu, click on **Administration**, and then select **Admin** below it. The current list of Administrator(s) shows up.



Admin Name	Privilege	Configure
admin	Read/Write	Modify

Settings of the Administration table

Admin Name: The username of Administrators for the Content Security Gateway. The user **admin** cannot be removed.

Privilege: The privileges of Administrators (Admin or Sub Admin)

The username of the main Administrator is **Admin** with **read / write** privilege.

Sub Admin may be created by clicking **New Sub Admin**. Sub Admin have **read only** privilege.

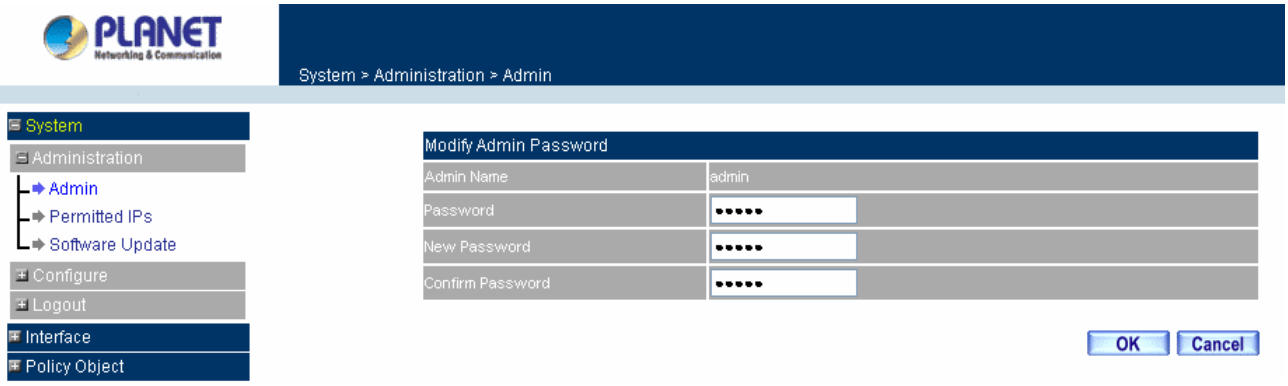
Configure: Click **Modify** to change the "Sub Admin" password and click **Remove** to delete a "Sub Admin".

Changing the Main/Sub-Admin's Password

Step 1. The **Modify Admin Password** window will appear. Enter in the required information:

- **Password:** enter original password.
- **New Password:** enter new password
- **Confirm Password:** enter the new password again.

Step 2. Click **OK** to confirm password change or click **Cancel** to cancel it.



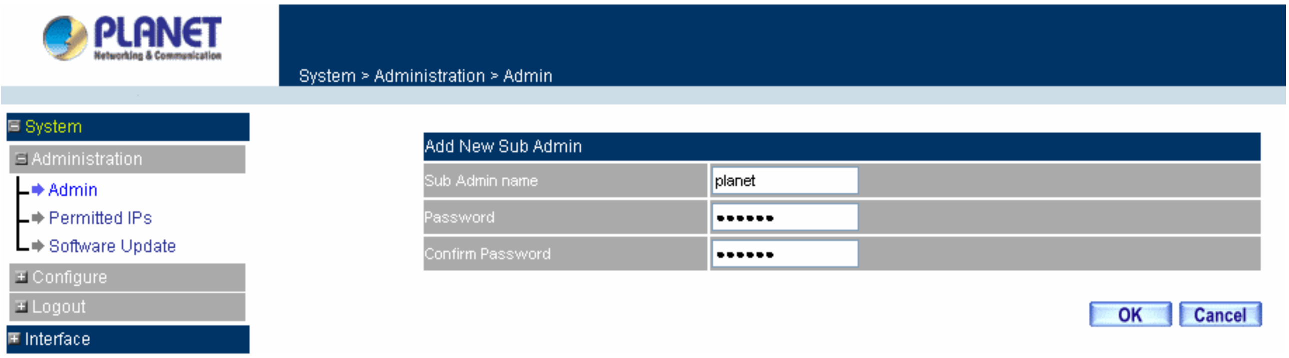
Modify Admin Password	
Admin Name	admin
Password	•••••
New Password	•••••
Confirm Password	•••••

Adding a new Sub Admin

Step 1. In the **Add New Sub Admin** window:

- **Sub Admin Name:** enter the username of new **Sub Admin.**
- **Password:** enter a password for the new **Sub Admin.**
- **Confirm Password:** enter the password again.

Step 2. Click **OK** to add the user or click **Cancel** to cancel the addition.

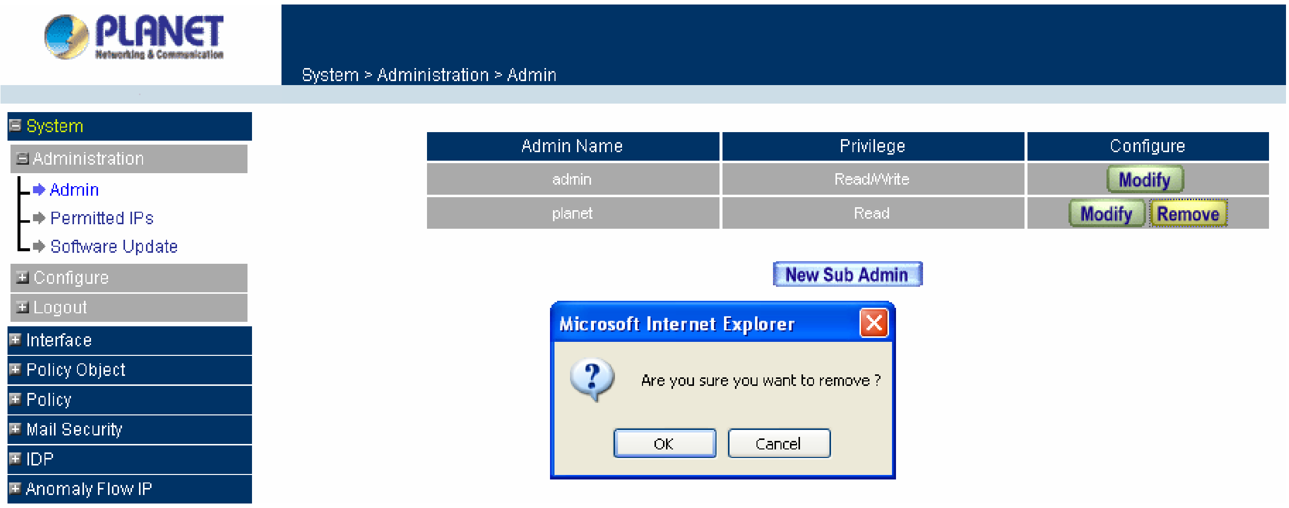


Add New Sub Admin	
Sub Admin name	planet
Password	••••••
Confirm Password	••••••

Removing a Sub Admin

Step 1. In the Administration table, locate the Admin name you want to edit, and click on the **Remove** option in the Configure field.

Step 2. The Remove confirmation pop-up box will appear. Click **OK** to remove that Sub Admin or click **Cancel** to cancel.

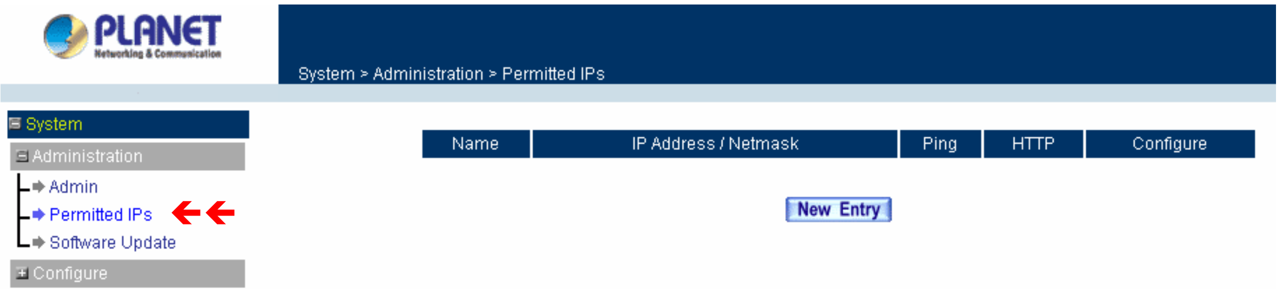


Admin Name	Privilege	Configure
admin	Read/Write	Modify
planet	Read	Modify Remove

Are you sure you want to remove ?

4.1.2 Permitted IPs

Only the authorized IP address is permitted to manage the Content Security Gateway.



Name	IP Address / Netmask	Ping	HTTP	Configure

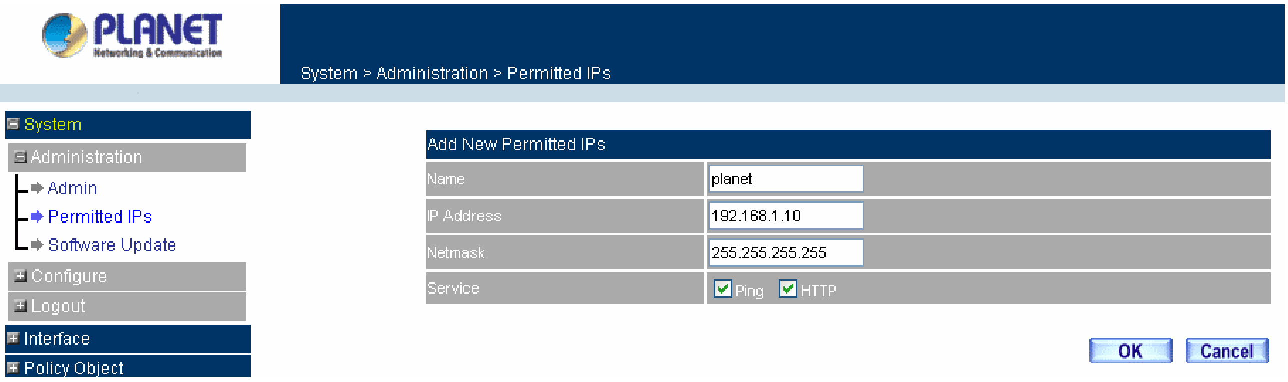
Add Permitted IPs Address

Step 1. Click **New Entry** button.

Step 2. In IP Address field, enter the LAN IP address or WAN IP address.

- **Name**: Enter the host name for the authorized IP address.
- **IP Address**: Enter the LAN IP address or WAN IP address.
- **Netmask**: Enter the netmask of LAN/WAN.
- **Ping**: Select this to allow the external network to ping the IP Address of the Firewall.
- **HTTP**: Check this item, Web User can use HTTP to connect to the Setting window of Content Security Gateway.

Step 3. Click **OK** to add Permitted IP or click **Cancel** to discard changes.



Add New Permitted IPs

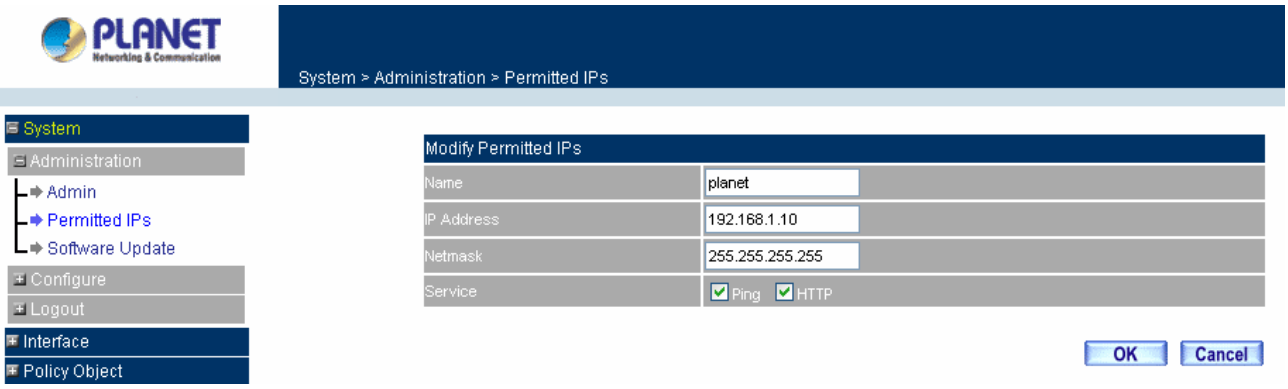
Name	planet
IP Address	192.168.1.10
Netmask	255.255.255.255
Service	☑ Ping ☑ HTTP

Modify Permitted IPs Address

Step 1. In the table of **Permitted IPs**, highlight the IP you want to modify, and then click **Modify**.

Step 2. In **Modify Permitted IPs**, enter new IP address.

Step 3. Click **OK** to modify or click **Cancel** to discard changes.



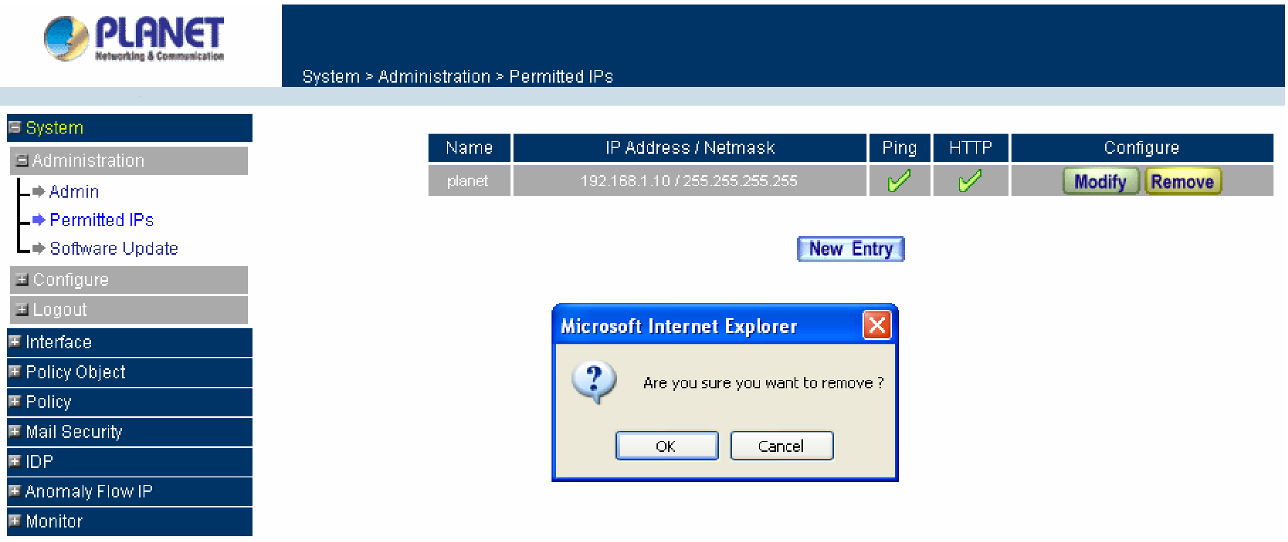
Modify Permitted IPs

Name	planet
IP Address	192.168.1.10
Netmask	255.255.255.255
Service	☑ Ping ☑ HTTP

Remove Permitted IPs Addresses

Step 1. In the table of **Permitted IPs**, highlight the IP you want to remove, and then click **Remove**.

Step 2. In the confirm window, click **OK** to remove or click **Cancel** to discard changes.



Name	IP Address / Netmask	Ping	HTTP	Configure
planet	192.168.1.10 / 255.255.255.255	✓	✓	Modify Remove

Microsoft Internet Explorer

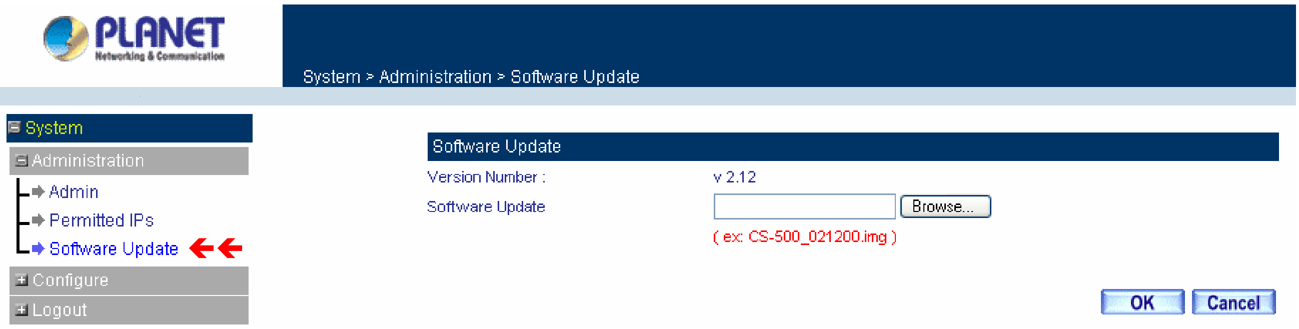
Are you sure you want to remove ?

4.1.3 Software Update

Under **Software Update**, the admin may update the device's software with a newer software. You may acquire the current version number of software in **Version Number**. Administrators may visit distributor's web site to download the latest version and save it in server's hard disk.

Step 1. Click **Browse** to select the latest version of Software.

Step 2. Click **OK** to update software.



Software Update

Version Number : v 2.12

Software Update

(ex: CS-500_021200.img)

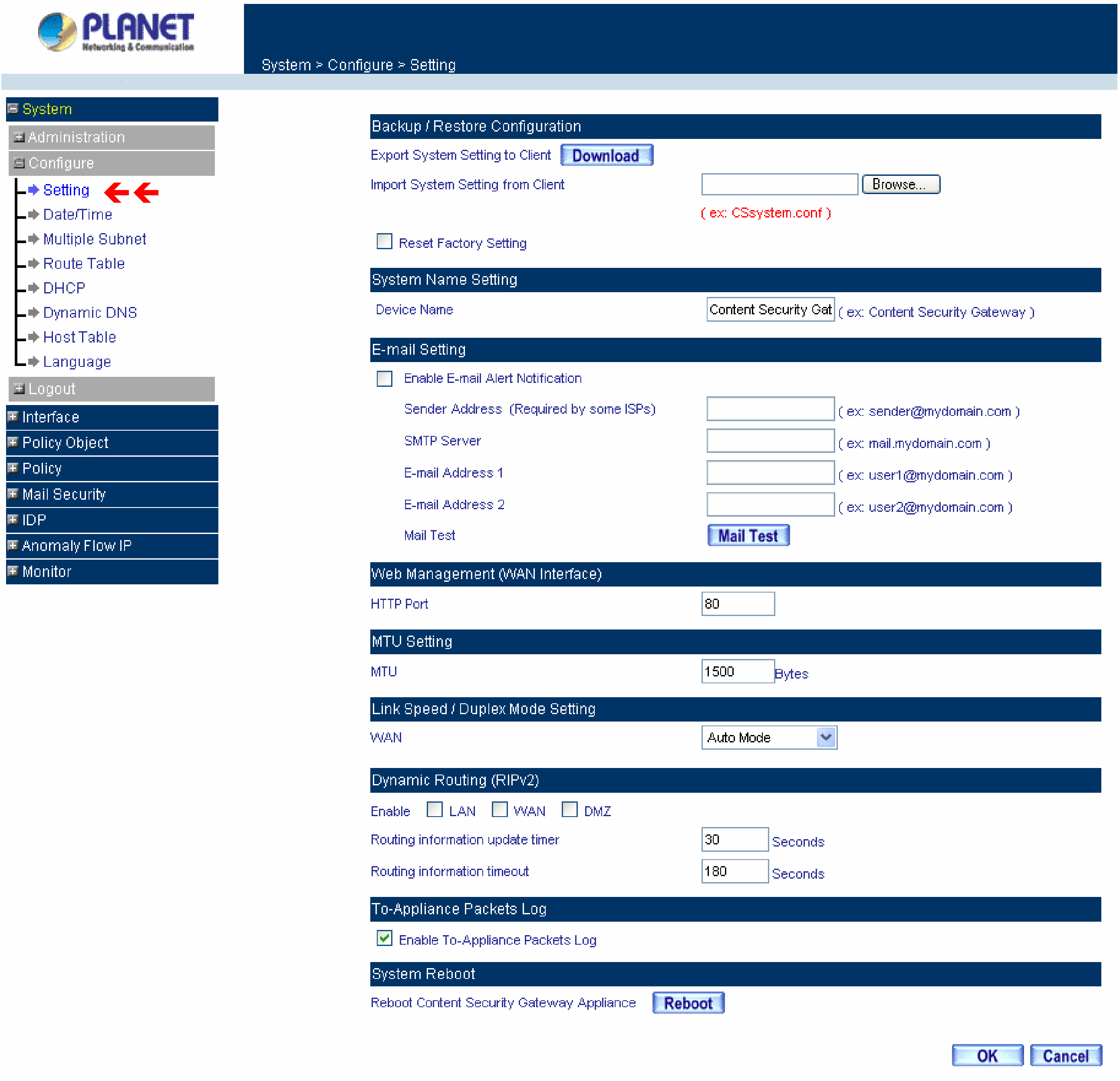
NOTE: It takes three minutes to update the software. The system will restart automatically after updating the software.

4.1.4 Setting

The Administrator may use this function to backup Content Security Gateway configurations and export (save) them to an **"Administrator"** computer or anywhere on the network; or restore a configuration file to the device; or restore the Content Security Gateway back to default factory settings.

Entering the Settings window

Click **Setting** in the **Configure** menu to enter the **Settings** window. The **Setting** will be shown on the screen.



System > Configure > Setting

Backup / Restore Configuration

Export System Setting to Client [Download]

Import System Setting from Client [ ] [Browse...]

(ex: CSsystem.conf)

□ Reset Factory Setting

System Name Setting

Device Name: Content Security Gat (ex: Content Security Gateway)

E-mail Setting

□ Enable E-mail Alert Notification

Sender Address (Required by some ISPs) (ex: sender@mydomain.com)

SMTP Server (ex: mail.mydomain.com)

E-mail Address 1 (ex: user1@mydomain.com)

E-mail Address 2 (ex: user2@mydomain.com)

Mail Test [Mail Test]

Web Management (WAN Interface)

HTTP Port: 80

MTU Setting

MTU: 1500 Bytes

Link Speed / Duplex Mode Setting

WAN: Auto Mode

Dynamic Routing (RIPv2)

Enable □ LAN □ WAN □ DMZ

Routing information update timer: 30 Seconds

Routing information timeout: 180 Seconds

To-Appliance Packets Log

☑ Enable To-Appliance Packets Log

System Reboot

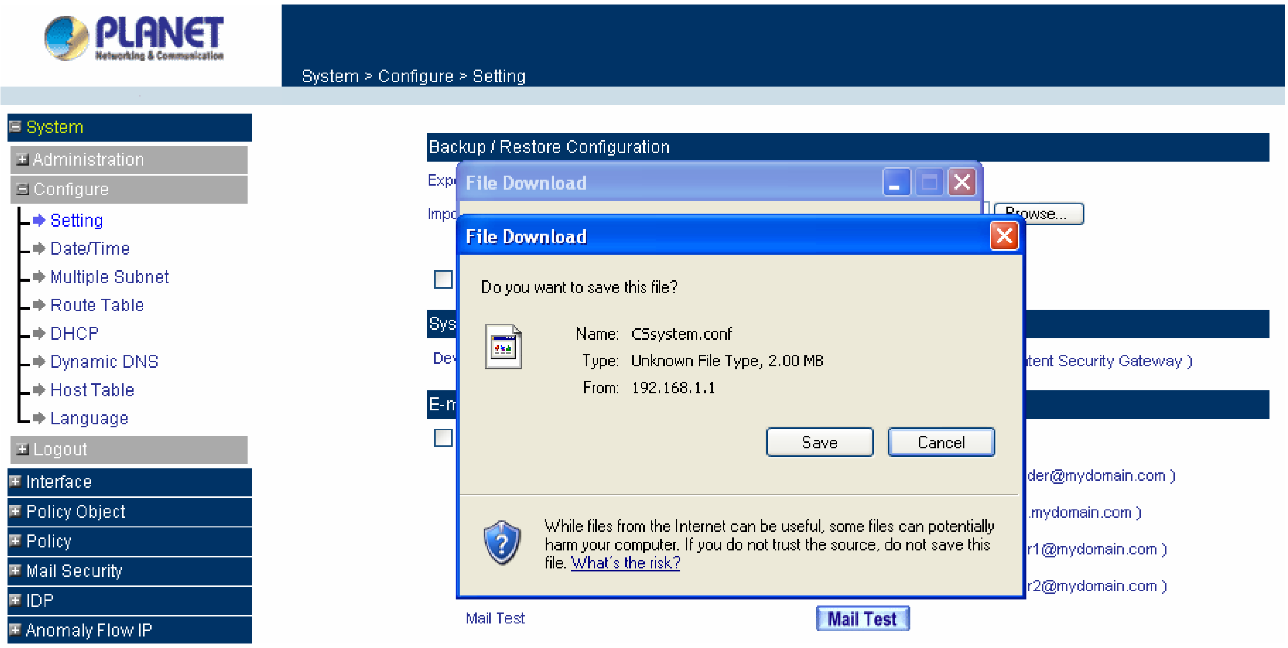
Reboot Content Security Gateway Appliance [Reboot]

[OK] [Cancel]

Exporting Content Security Gateway settings

Step 1. Under **Backup/Restore Configuration**, click on the **Download** button next to **Export System Settings to Client**.

Step 2. When the **File Download** pop-up window appears, choose the destination place to save the exported file. The **Administrator** may choose to rename the file if preferred.



File Download

Do you want to save this file?

Name: CSsystem.conf
Type: Unknown File Type, 2.00 MB
From: 192.168.1.1

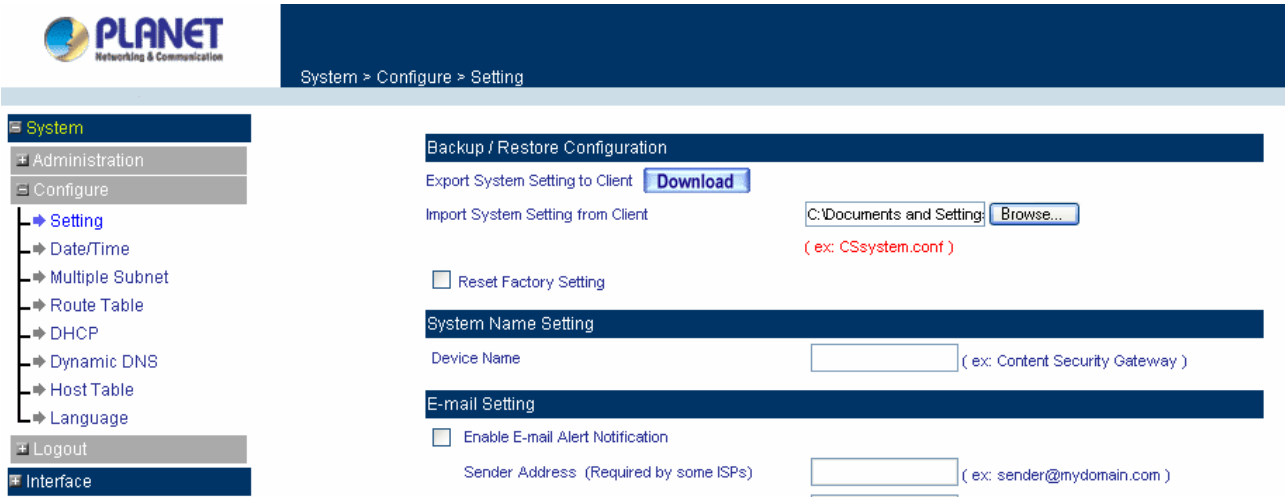
Save | Cancel

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not save this file. What's the risk?

Importing Content Security Gateway settings

Under **Backup/Restore Configuration**, click on the **Browse** button next to **Import System Settings from Client**. When the **Choose File** pop-up window appears, select the file which contains the saved Content Security Gateway Settings, then click **OK**.

Click **OK** to import the file into the **Content Security Gateway** or click **Cancel** to cancel importing.



Backup / Restore Configuration

Export System Setting to Client [Download]

Import System Setting from Client C:\Documents and Setting [Browse...]

(ex: CSsystem.conf)

□ Reset Factory Setting

System Name Setting

Device Name (ex: Content Security Gateway)

E-mail Setting

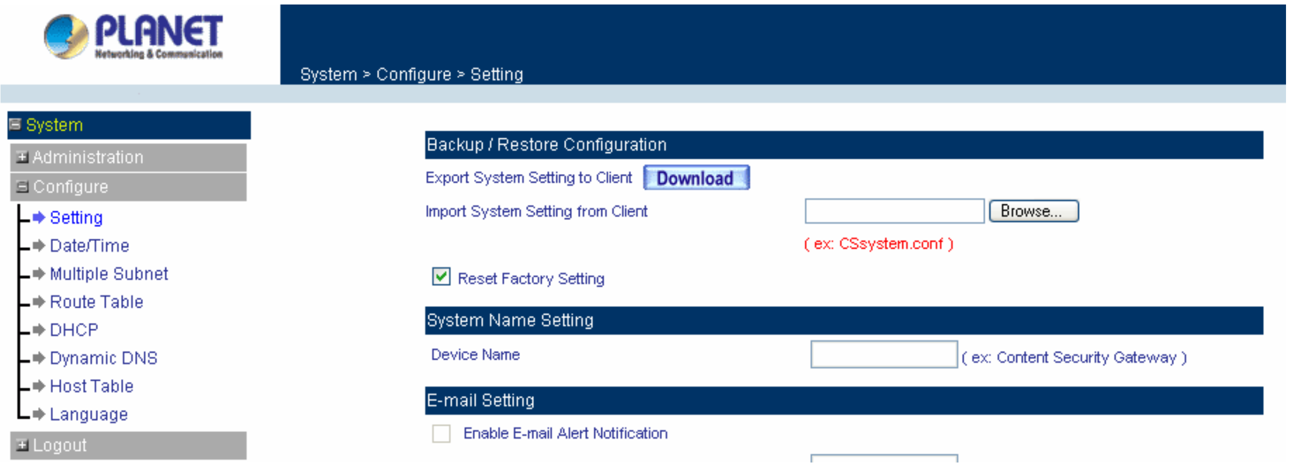
□ Enable E-mail Alert Notification

Sender Address (Required by some ISPs) (ex: sender@mydomain.com)

Restoring Factory Default Settings

Step 1. Select **Reset Factory Settings** under **Backup/Restore Configuration**.

Step 2. Click **OK** at the bottom-right of the screen to restore the factory settings.



Backup / Restore Configuration

Export System Setting to Client

Import System Setting from Client (ex: CSsystem.conf)

☑ Reset Factory Setting

System Name Setting

Device Name (ex: Content Security Gateway)

E-mail Setting

□ Enable E-mail Alert Notification

System Name Setting

Input the name you want into **Device Name** column to be the device name.

Email Setting

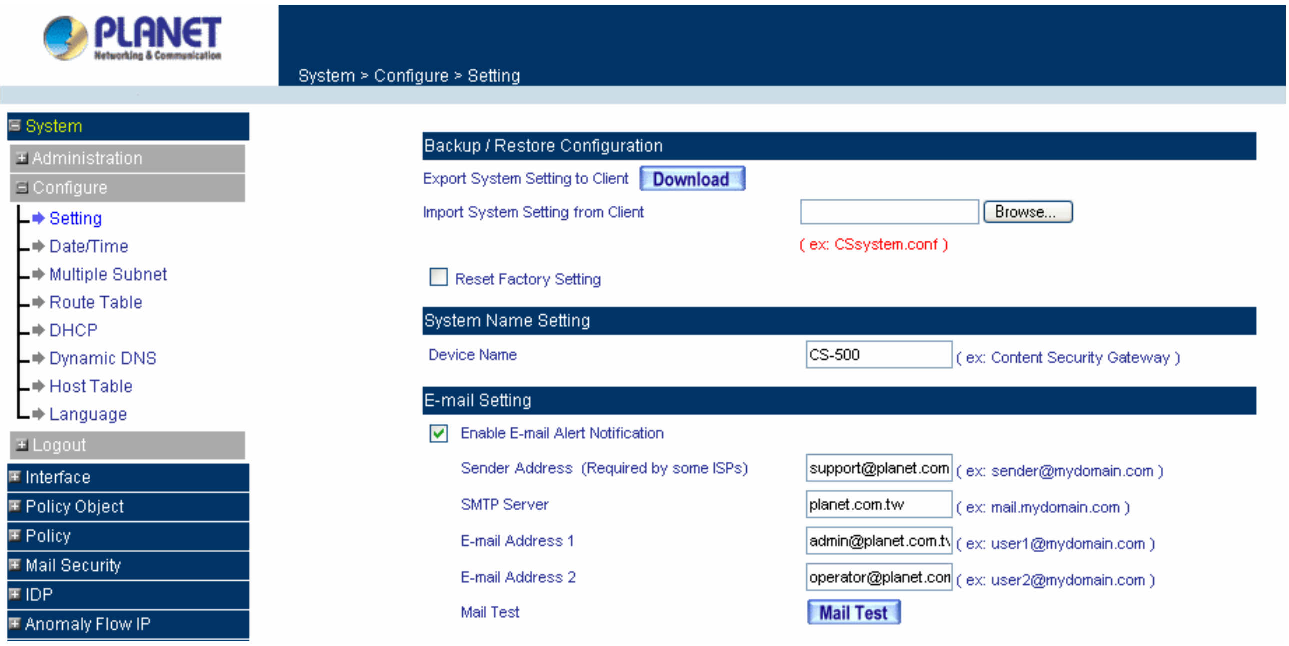
Step 1. Select **Enable E-mail Alert Notification** under **E-Mail Setting**. This function will enable the Content Security Gateway to send e-mail alerts to the System Administrator when the network is being attacked by hackers or when emergency conditions occur.

Step 2. **SMTP Server IP:** Enter SMTP server's IP address.

Step 3. **E-Mail Address 1:** Enter the first e-mail address to receive the alarm notification.

Step 4. **E-Mail Address 2:** Enter the second e-mail address to receive the alarm notification. (Optional)

Click **OK** on the bottom-right of the screen to enable E-mail alert notification.



Backup / Restore Configuration

Export System Setting to Client

Import System Setting from Client (ex: CSsystem.conf)

□ Reset Factory Setting

System Name Setting

Device Name: CS-500 (ex: Content Security Gateway)

E-mail Setting

☑ Enable E-mail Alert Notification

Sender Address (Required by some ISPs): support@planet.com (ex: sender@mydomain.com)

SMTP Server: planet.com.tw (ex: mail.mydomain.com)

E-mail Address 1: admin@planet.com.tv (ex: user1@mydomain.com)

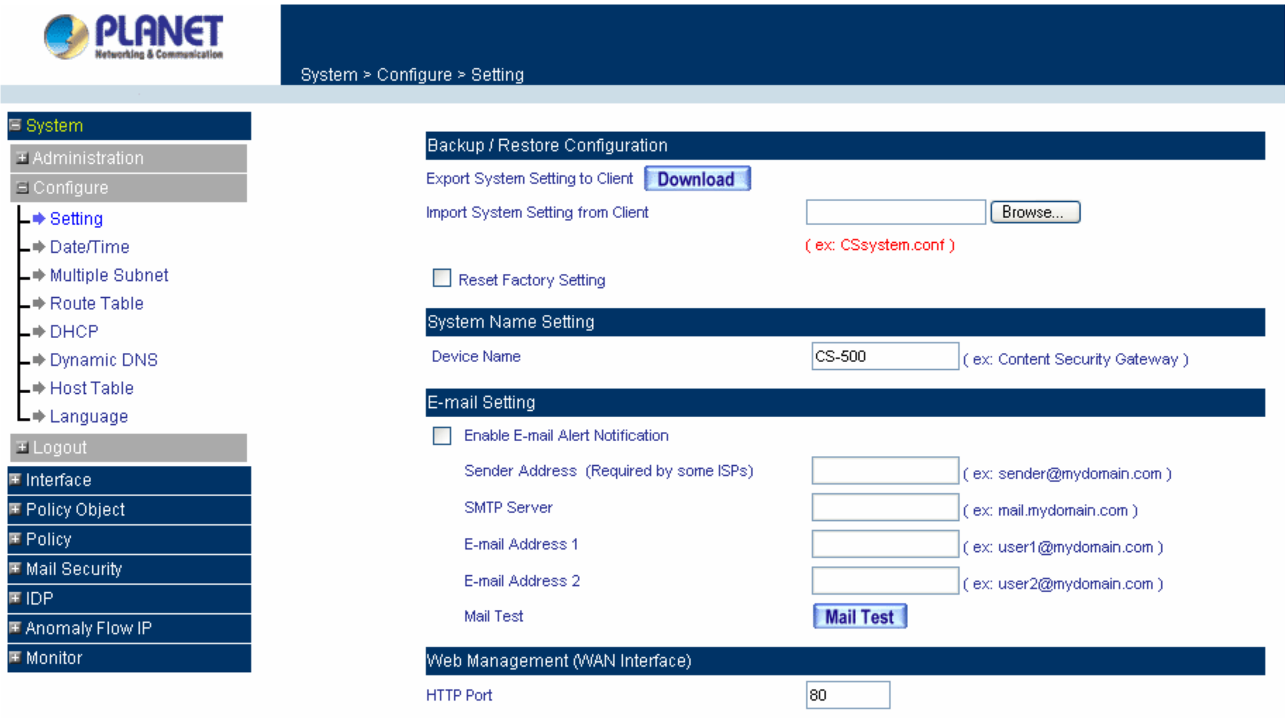
E-mail Address 2: operator@planet.com (ex: user2@mydomain.com)

Mail Test

Web Management (WAN Interface)

The administrator can change the port number used by HTTP port1 anytime. (Remote UI Management)

Step 1. **Set Web Management (WAN Interface).** The administrator can change the port number used by HTTP port anytime.



Backup / Restore Configuration

Export System Setting to Client

Import System Setting from Client (ex: CSsystem.conf)

□ Reset Factory Setting

System Name Setting

Device Name: CS-500 (ex: Content Security Gateway)

E-mail Setting

□ Enable E-mail Alert Notification

Sender Address (Required by some ISPs) (ex: sender@mydomain.com)

SMTP Server (ex: mail.mydomain.com)

E-mail Address 1 (ex: user1@mydomain.com)

E-mail Address 2 (ex: user2@mydomain.com)

Mail Test

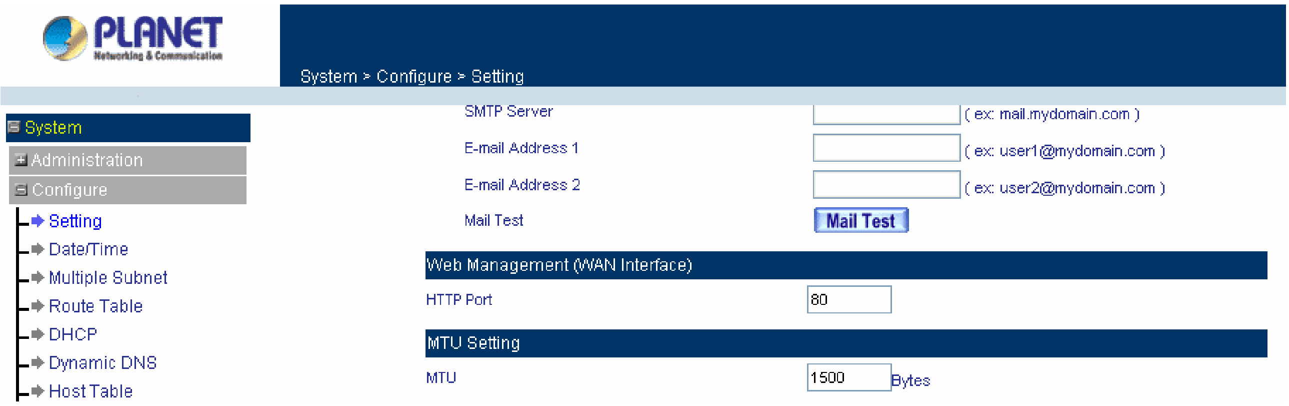
Web Management (WAN Interface)

HTTP Port: 80

MTU (set networking packet length)

The administrator can modify the networking packet length.

Step 1. **MTU Setting.** Modify the networking packet length.



SMTP Server (ex: mail.mydomain.com)

E-mail Address 1 (ex: user1@mydomain.com)

E-mail Address 2 (ex: user2@mydomain.com)

Mail Test

Web Management (WAN Interface)

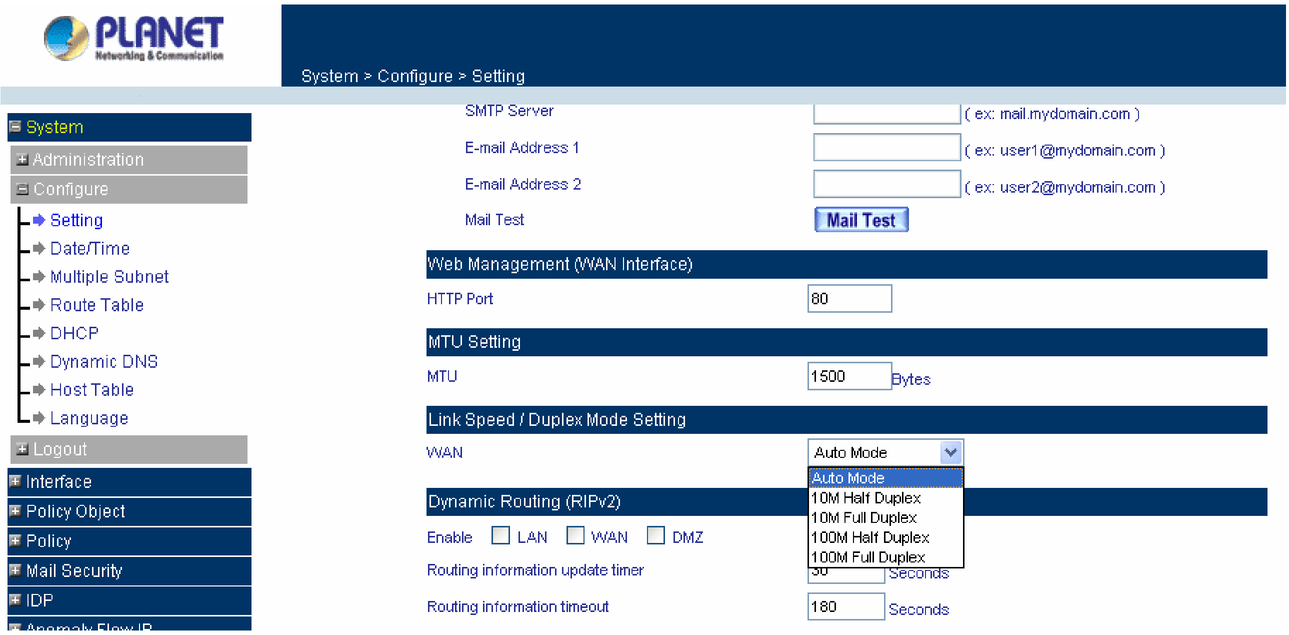
HTTP Port: 80

MTU Setting

MTU: 1500 Bytes

Link Speed / Duplex Mode Setting

This function allows administrator to set the transmission speed and mode of WAN Port.



SMTP Server (ex: mail.mydomain.com)

E-mail Address 1 (ex: user1@mydomain.com)

E-mail Address 2 (ex: user2@mydomain.com)

Mail Test

Web Management (WAN Interface)

HTTP Port 80

MTU Setting

MTU 1500 Bytes

Link Speed / Duplex Mode Setting

WAN Auto Mode

- Auto Mode
- 10M Half Duplex
- 10M Full Duplex
- 100M Half Duplex
- 100M Full Duplex

Dynamic Routing (RIPv2)

Enable □ LAN □ WAN □ DMZ

Routing information update timer 30 Seconds

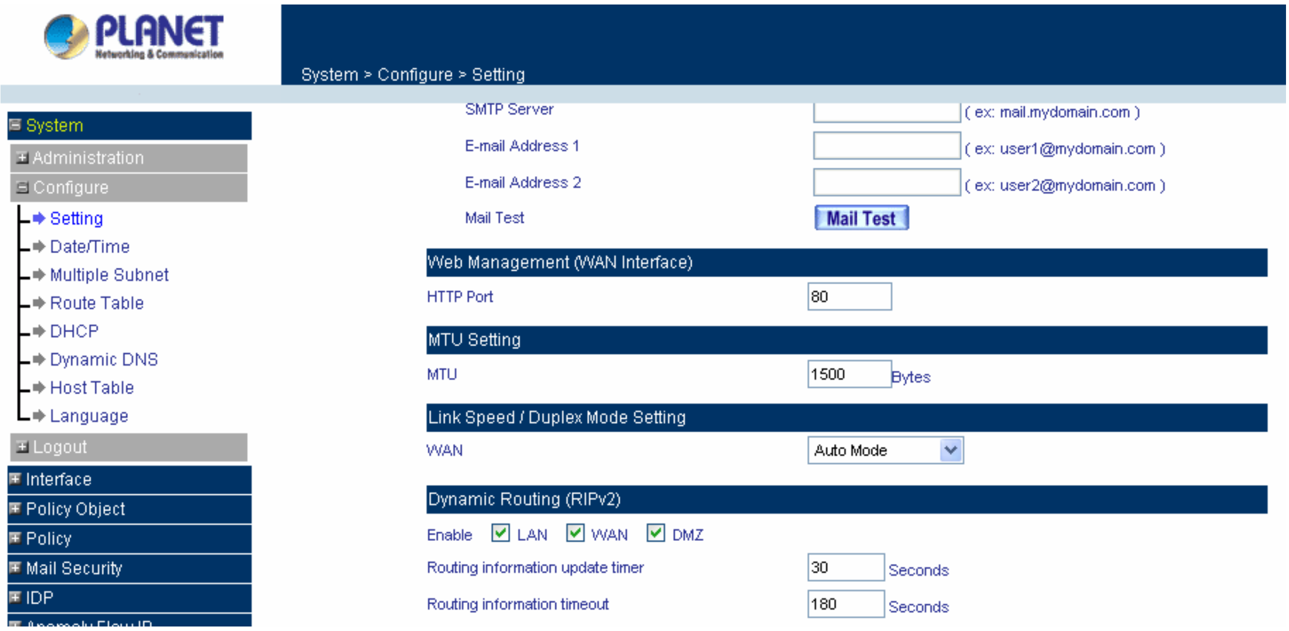
Routing information timeout 180 Seconds

Dynamic Routing (RIPv2)

Enable Dynamic Routing (RIPv2), CS-500 will advertise an IP address pool to the specific network so that the address pool can be provided to the network. You can choose to enable LAN, WAN or DMZ interface to allow RIP protocol supporting.

Routing information update timer: CS-500 will send out the RIP protocol in a period of time to update the routing table, the default timer is 30 seconds.

Routing information timeout: If CS-500 does not receive the RIP protocol from the other router in a period of time, CS-500 will cut off the routing automatically until it receives RIP protocol again. The default timer is 180 seconds.



SMTP Server (ex: mail.mydomain.com)

E-mail Address 1 (ex: user1@mydomain.com)

E-mail Address 2 (ex: user2@mydomain.com)

Mail Test

Web Management (WAN Interface)

HTTP Port 80

MTU Setting

MTU 1500 Bytes

Link Speed / Duplex Mode Setting

WAN Auto Mode

Dynamic Routing (RIPv2)

Enable ☑ LAN ☑ WAN ☑ DMZ

Routing information update timer 30 Seconds

Routing information timeout 180 Seconds

To-Appliance Packet Logging

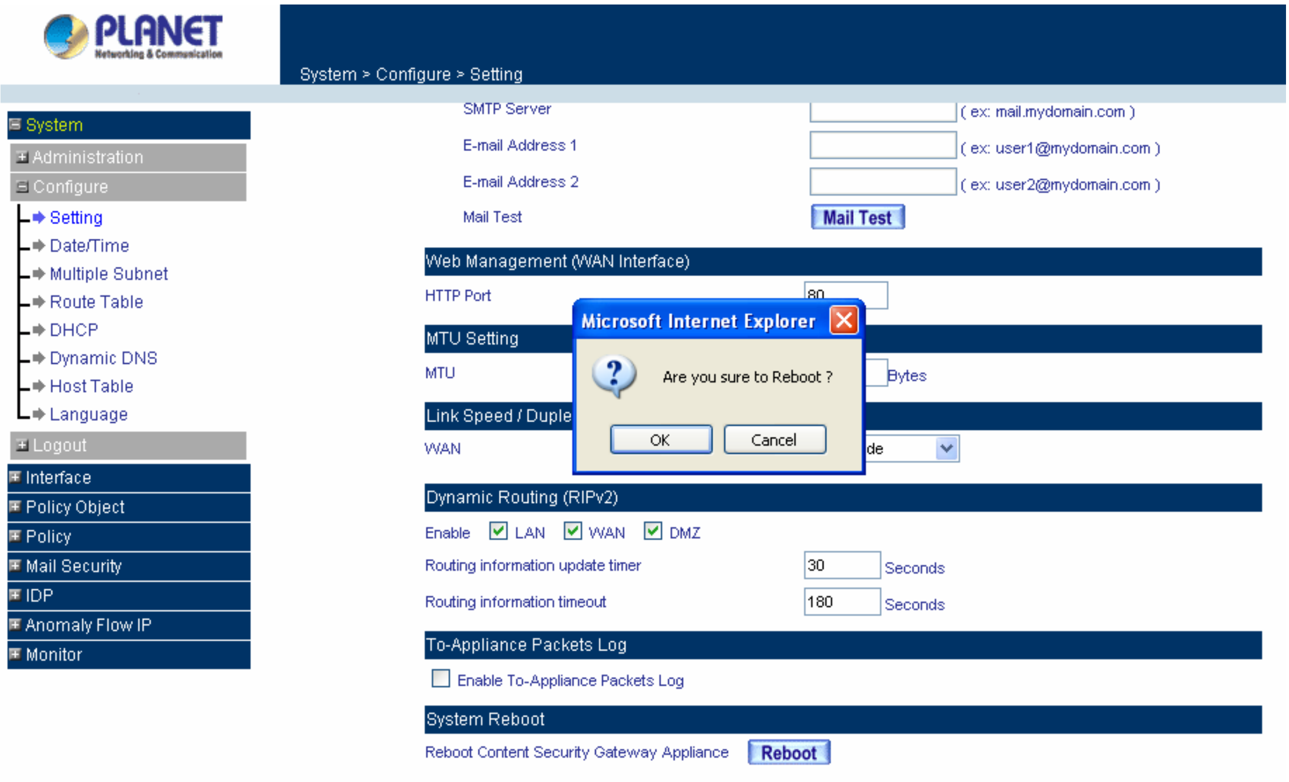
When the function is selected, the CS-500 will record the packets that contain the IP address of CS-500 in source or destination, the records will display in Traffic Log for administrator to inquire about.

System Reboot

Once this function is enabled, the Content Security Gateway will be rebooted**.**

Reboot Appliance: Click **Reboot.**

A confirmation pop-up box will appear. Follow the confirmation pop-up box, click **OK** to restart Content Security Gateway or click **Cancel** to discard changes.



SMTP Server (ex: mail.mydomain.com)

E-mail Address 1 (ex: user1@mydomain.com)

E-mail Address 2 (ex: user2@mydomain.com)

Mail Test

Web Management (WAN Interface)

HTTP Port 80

MTU Setting

MTU Bytes

Link Speed / Duple

WAN de

Are you sure to Reboot ?

Dynamic Routing (RIPv2)

Enable ☑ LAN ☑ WAN ☑ DMZ

Routing information update timer 30 Seconds

Routing information timeout 180 Seconds

To-Appliance Packets Log

□ Enable To-Appliance Packets Log

System Reboot

Reboot Content Security Gateway Appliance

4.1.5 Date/Time

Synchronizing the Content Security Gateway with the System Clock

Administrator can configure the Content Security Gateway's date and time by either syncing to an Internet Network Time Server (NTP) or by syncing to your computer's clock.

Follow these steps to sync to an Internet Time Server

Step 1. Enable synchronization by checking the box.

Step 2. Click the down arrow to select the offset time from GMT.

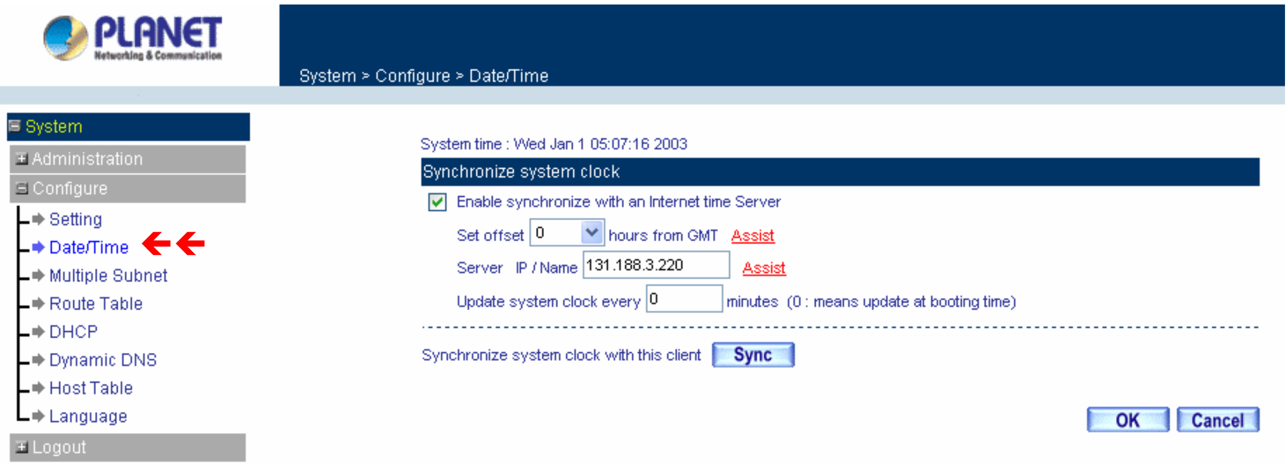
Step 3. Enter the Server IP Address or Server name with which you want to synchronize.

Step 4. Update system clock every □ minutes You can set the interval time to synchronize with outside servers. If you set it to 0, it means the device will not synchronize automatically.

Follow this step to sync to your computer's clock.

Step 1. Click on the **Sync** button.

Click **OK** to apply the setting or click **Cancel** to discard changes.



System time : Wed Jan 1 05:07:16 2003

Synchronize system clock

☑ Enable synchronize with an Internet time Server

Set offset 0 hours from GMT

Server IP / Name 131.188.3.220

Update system clock every 0 minutes (0 : means update at booting time)

Synchronize system clock with this client

4.1.6 Multiple Subnet

NAT mode

Multiple Subnet allows local port to set multiple subnet works and connect with the Internet through WAN IP Addresses.

For instance: The lease line of a company applies several real IP Addresses 168.85.88.0/24, and the company is divided into R&D department, service, sales department, procurement department, accounting department, the company can distinguish each department by different subnet works for the purpose of convenient management. The settings are as the following:

1. R&D department sub-network: 192.168.1.11/24 (LAN) ←→ 168.85.88.253 (WAN)
2. Service department sub-network: 192.168.2.11/24 (LAN) ←→ 168.85.88.252 (WAN)
3. Sales department sub-network: 192.168.3.11/24 (LAN) ←→ 168.85.88.251 (WAN)
4. Procurement department sub-network: 192.168.4.11/24 (LAN) ←→ 168.85.88.250(WAN)
5. Accounting department sub-network: 192.168.5.11/24 (LAN) ←→ 168.85.88.249 (WAN)

The first department (R&D department) was set while setting interface IP, the other four ones have to be added in Multiple Subnet, after completing the settings, each department use the different WAN IP address to connect to the internet. The settings of LAN computers on Service department are as the following:

Service IP Address: 192.168.2.1

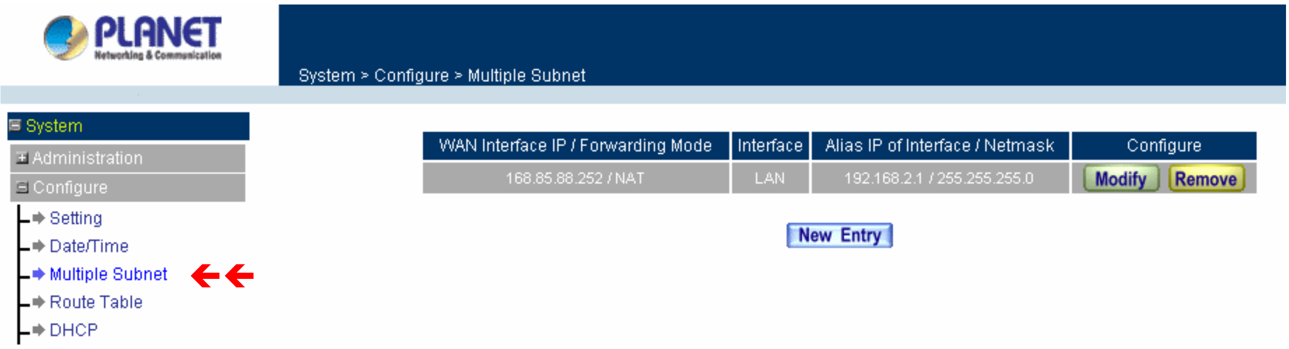
Subnet Mask: 255.255.255.0

Default Gateway: 192.168.2.11

The other departments are also set by groups, this is the function of Multiple Subnet.

Multiple Subnet settings

Click **System** on the left side menu bar, select **Configure** then click **Multiple Subnet** to enter Multiple Subnet window.



System > Configure > Multiple Subnet

WAN Interface IP / Forwarding Mode	Interface	Alias IP of Interface / Netmask	Configure
168.85.88.252 / NAT	LAN	192.168.2.1 / 255.255.255.0	Modify Remove

Multiple Subnet functions

WAN Interface IP / Forwarding Mode: Display WAN Port IP address and Forwarding Mode.

Interface: Indicate the multiple subnet location in LAN or DMZ site.

Alias IP of Int. Interface / Netmask: Local port IP address and subnet Mask.

Configure: Modify the settings of Multiple Subnet. Click Modify to modify the parameters of Multiple Subnet or click Delete to delete settings.

Add a Multiple Subnet NAT Mode.

Step 1: Click the **New Entry** button below to add Multiple Subnet.

Step 2: Enter the IP address in the website name column of the new window.

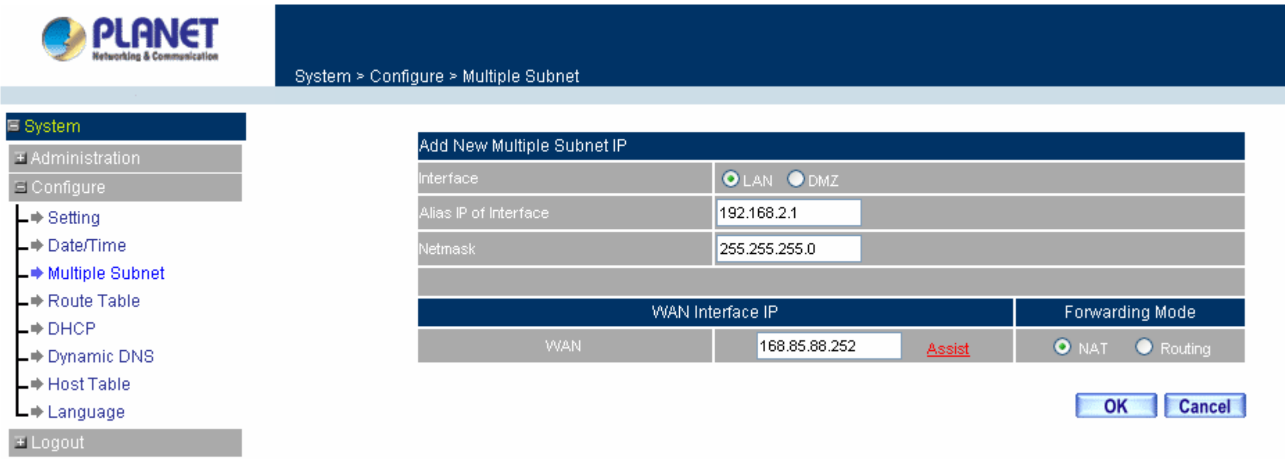
Alias IP of LAN Interface: Enter Local port IP address.

Netmask: Enter Local port subnet Mask.

WAN Interface IP: Add WAN IP.

Forwarding Mode: Click the NAT button below to setup.

Step 3: Click OK to add Multiple Subnet or click Cancel to discard changes.



System > Configure > Multiple Subnet

Add New Multiple Subnet IP

Interface	● LAN ○ DMZ
Alias IP of Interface	192.168.2.1
Netmask	255.255.255.0

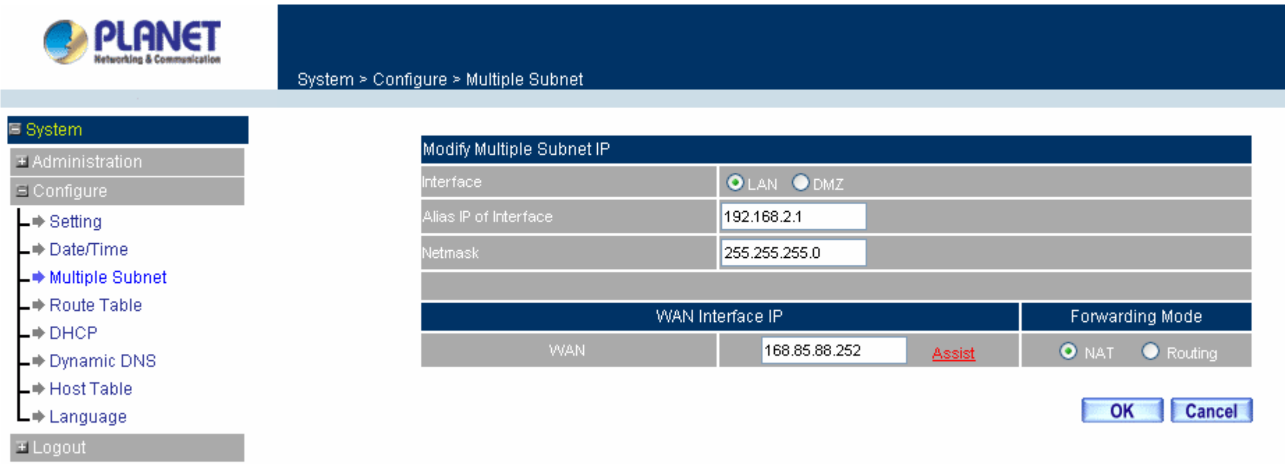
WAN Interface IP		Forwarding Mode
WAN	168.85.88.252 Assist	● NAT ○ Routing

Modify a Multiple Subnet

Step 1: Find the IP address you want to modify and click Modify.

Step 2: Enter the new IP address in Modify Multiple Subnet window.

Step 3: Click the OK button below to change the setting or click Cancel to discard changes.



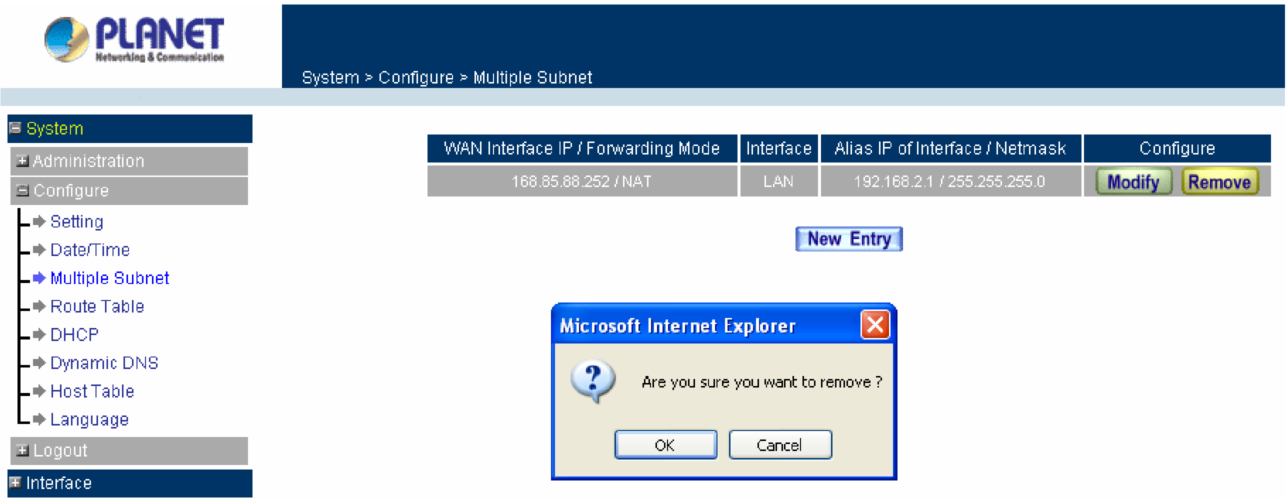
Modify Multiple Subnet IP	
Interface	● LAN ○ DMZ
Alias IP of Interface	192.168.2.1
Netmask	255.255.255.0

WAN Interface IP		Forwarding Mode
WAN	168.85.88.252	● NAT ○ Routing

Removing a Multiple Subnet

Step 1: Find the IP address you want to delete and click Delete.

Step 2: A confirmation pop-up box will appear, click OK to delete the setting or click Cancel to discard changes.



WAN Interface IP / Forwarding Mode	Interface	Alias IP of Interface / Netmask	Configure
168.85.88.252 / NAT	LAN	192.168.2.1 / 255.255.255.0	Modify Remove

Are you sure you want to remove ?

Routing Mode

Multiple Subnet allows local port to set Multiple Subnet Routing Mode and connect with the internet through WAN IP address.

For example, the leased line of a company applies several real IP Addresses 168.85.88.0/24 and the company is divided into R&D, Customer Service, Sales, Procurement, and Accounting Department. The company can distinguish each department by different sub-network for the purpose of convenient management.

The settings are as the following:

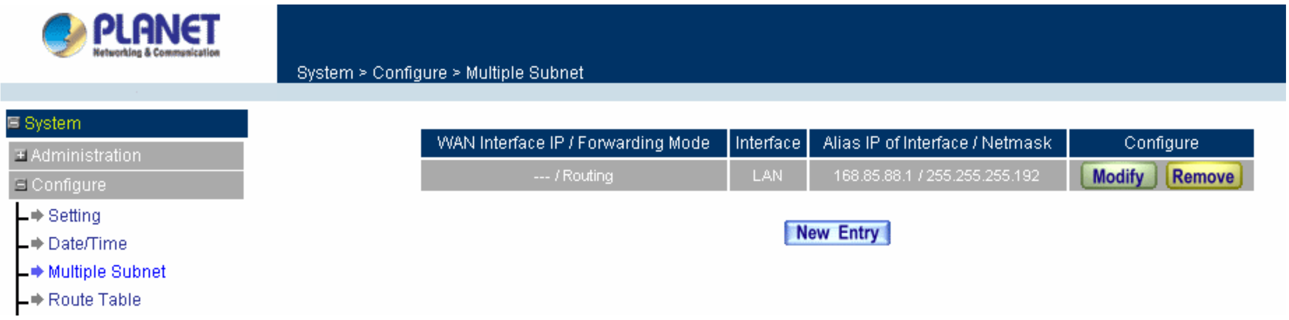
R&D: Alias IP of LAN interface - 168.85.88.1, Netmask: 255.255.255.192

Sales: Alias IP of LAN interface - 168.85.88.65, Netmask: 255.255.255.192

Procurement: Alias IP of LAN interface - 168.85.88.129, Netmask: 255.255.255.192

Accounting: Alias IP of LAN interface - 168.85.88.193, Netmask: 255.255.255.192

Click System on the left side menu bar, then click Multiple Subnet below Configure menu. Enter Multiple Subnet window.



WAN Interface IP / Forwarding Mode	Interface	Alias IP of Interface / Netmask	Configure
--- / Routing	LAN	168.85.88.1 / 255.255.255.192	Modify Remove

Multiple Subnet functions

WAN Interface IP / Forwarding Mode: Display WAN Port IP address and Forwarding Mode which is NAT Mode or Routing Mode.

Interface: Indicate the multiple subnet location in LAN or DMZ site.

Alias IP of Int. Interface / Netmask: Local port IP address and subnet Mask.

Configure: Modify the settings of Multiple Subnet. Click Modify to modify the parameters of Multiple Subnet or click Delete to delete settings.

Adding a Multiple Subnet Routing Mode

Step 1: Click the Add button below to add Multiple Subnet.

Step 2: Enter the IP address in Add Multiple Subnet window.

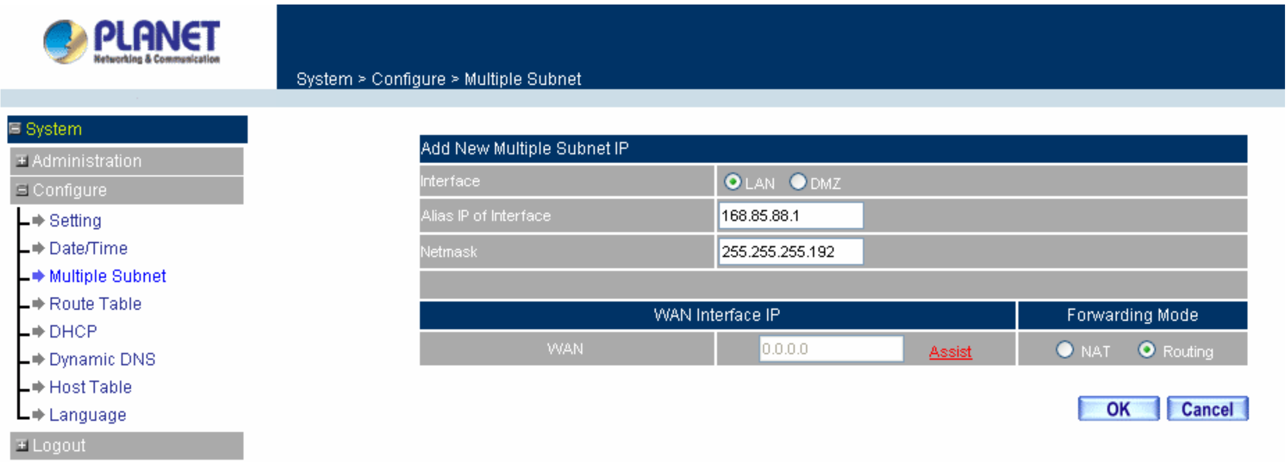
Alias IP of LAN Interface: Enter Local port IP Address.

Netmask: Enter Local port subnet Mask.

WAN Interface IP: Add WAN IP

Forwarding Mode: Click the Routing button below to setup.

Step 3: Click OK to add Multiple Subnet or click Cancel to discard changes.

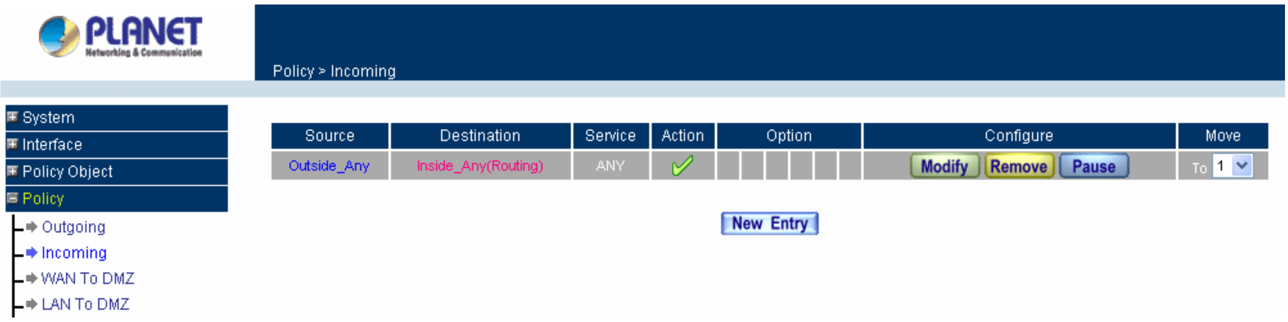


Add New Multiple Subnet IP

Interface	● LAN ○ DMZ
Alias IP of Interface	168.85.88.1
Netmask	255.255.255.192

WAN Interface IP		Forwarding Mode
WAN	0.0.0.0	○ NAT ● Routing

Step 4: Adding a new WAN to LAN Policy. In the Incoming window, click the New Entry button.



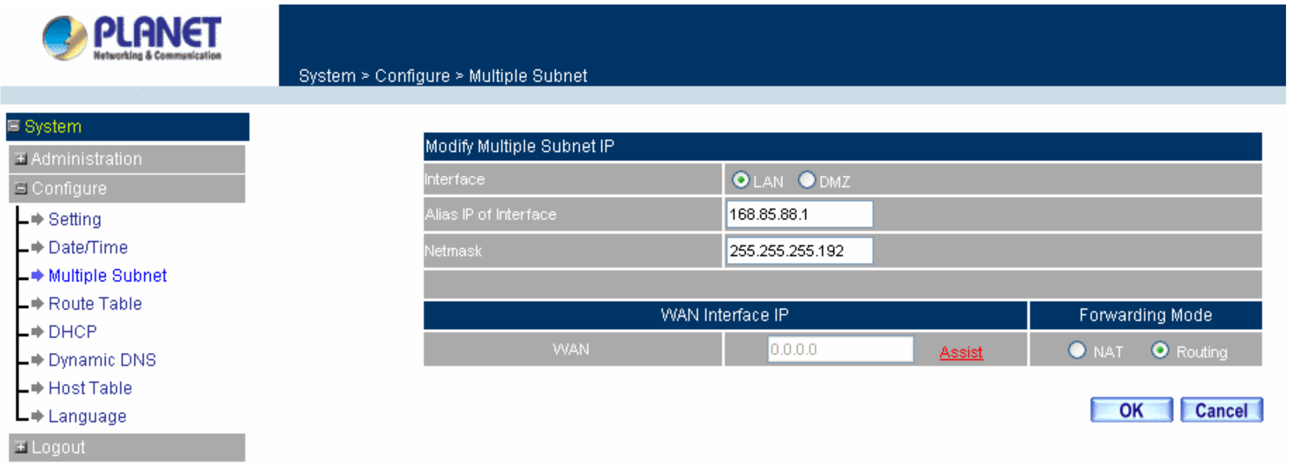
Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Inside_Any(Routing)	ANY	✓		Modify Remove Pause	To 1

Modify a Multiple Subnet Routing Mode

Step 1: Find the IP address you want to modify in Multiple Subnet menu, then click Modify button, on the right side of the service providers, click OK.

Step 2: Enter the new IP address in Modify Multiple Subnet window.

Step 3: Click the OK button below to change the setting or click Cancel to discard changes.



Modify Multiple Subnet IP

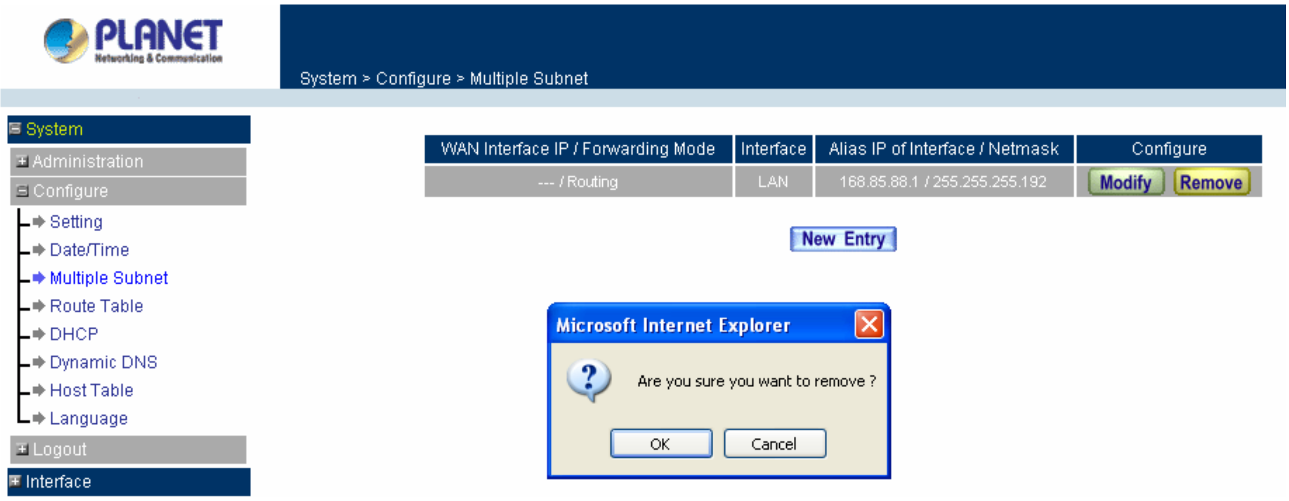
Interface	● LAN ○ DMZ
Alias IP of Interface	168.85.88.1
Netmask	255.255.255.192

WAN Interface IP		Forwarding Mode
WAN	0.0.0.0 Assist	○ NAT ● Routing

Removing a Multiple Subnet Routing Mode

Step 1: Find the IP Address you want to delete in Multiple Subnet menu, then click Delete button, on the right side of the service providers, click OK.

Step 2: A confirmation pop-up box will appear, click OK to delete the setting or click Cancel to discard changes.



WAN Interface IP / Forwarding Mode	Interface	Alias IP of Interface / Netmask	Configure
--- / Routing	LAN	168.85.88.1 / 255.255.255.192	Modify Remove

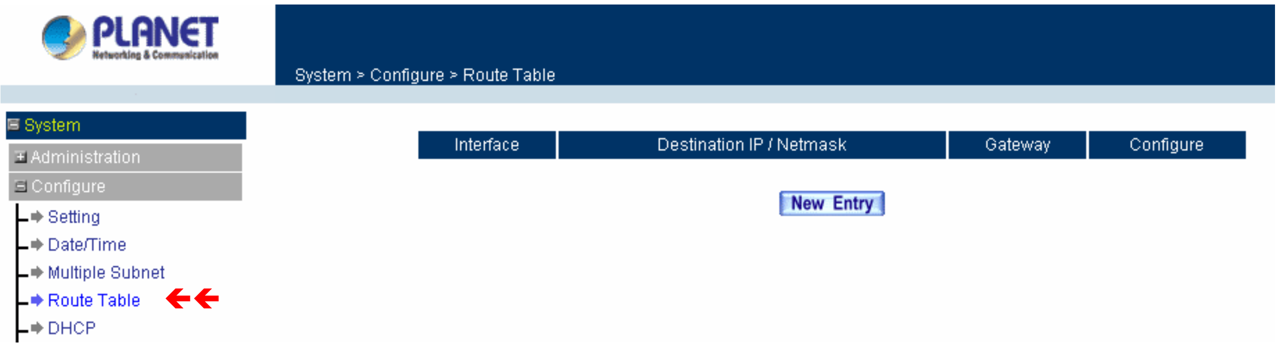
Are you sure you want to remove ?

4.1.7 Route Table

In this section, the Administrator can add static routes for the networks.

Entering the Route Table screen

Step 1. Click **System** on the left hand side menu bar, then click **Route Table** below the **Configure** menu. The Route Table window appears, in which current route settings are shown.



Interface	Destination IP / Netmask	Gateway	Configure

Route Table functions

- **Interface:** Destination network, LAN or WAN networks.
- **Destination IP / Netmask:** IP address and subnet mask of destination network.
- **Gateway:** Gateway IP address for connecting to destination network.
- **Configure:** Change settings in the route table.

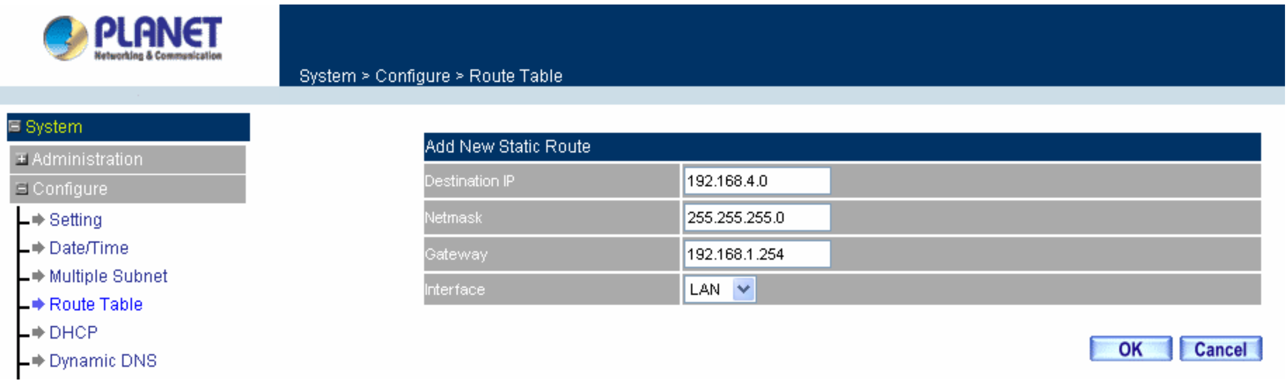
Adding a new Static Route

Step 1. In the Route Table window, click the **New Entry** button.

Step 2. In the Add New Static Route window, enter new static route information.

Step 3. In the Interface field's pull-down menu, choose the network to connect (LAN, WAN, DMZ).

Step 4. Click **OK** to add the new static route or click **Cancel** to cancel.



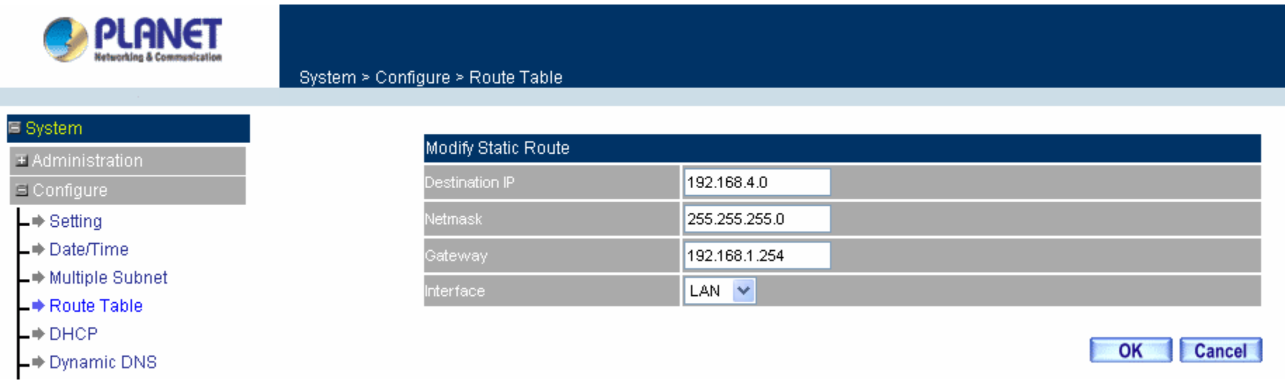
Add New Static Route	
Destination IP	192.168.4.0
Netmask	255.255.255.0
Gateway	192.168.1.254
Interface	LAN

Modifying a Static Route:

Step 1. In the Route Table menu, find the route to edit and click the corresponding Modify option in the Configure field.

Step 2. In the **Modify Static Route** window, modify the necessary routing addresses.

Step 3. Click **OK** to apply changes or click **Cancel** to cancel it.

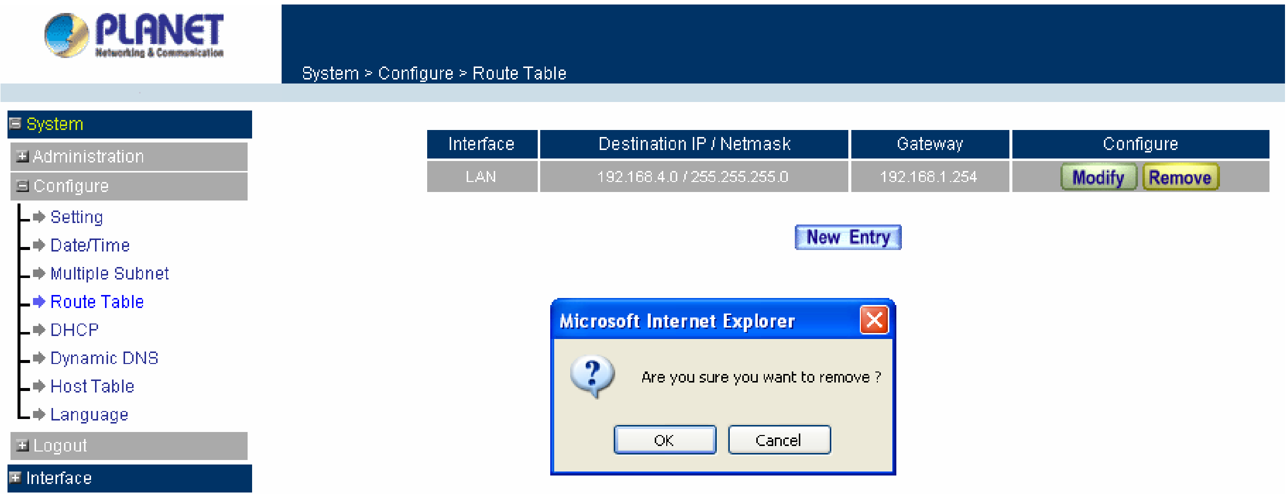


Modify Static Route	
Destination IP	192.168.4.0
Netmask	255.255.255.0
Gateway	192.168.1.254
Interface	LAN

Removing a Static Route

Step 1. In the Route Table window, find the route to remove and click the corresponding Remove option in the Configure field.

Step 2. In the Remove confirmation pop-up box, click **OK** to confirm removing or click **Cancel** to cancel it.



Interface	Destination IP / Netmask	Gateway	Configure
LAN	192.168.4.0 / 255.255.255.0	192.168.1.254	Modify Remove

Microsoft Internet Explorer

Are you sure you want to remove ?

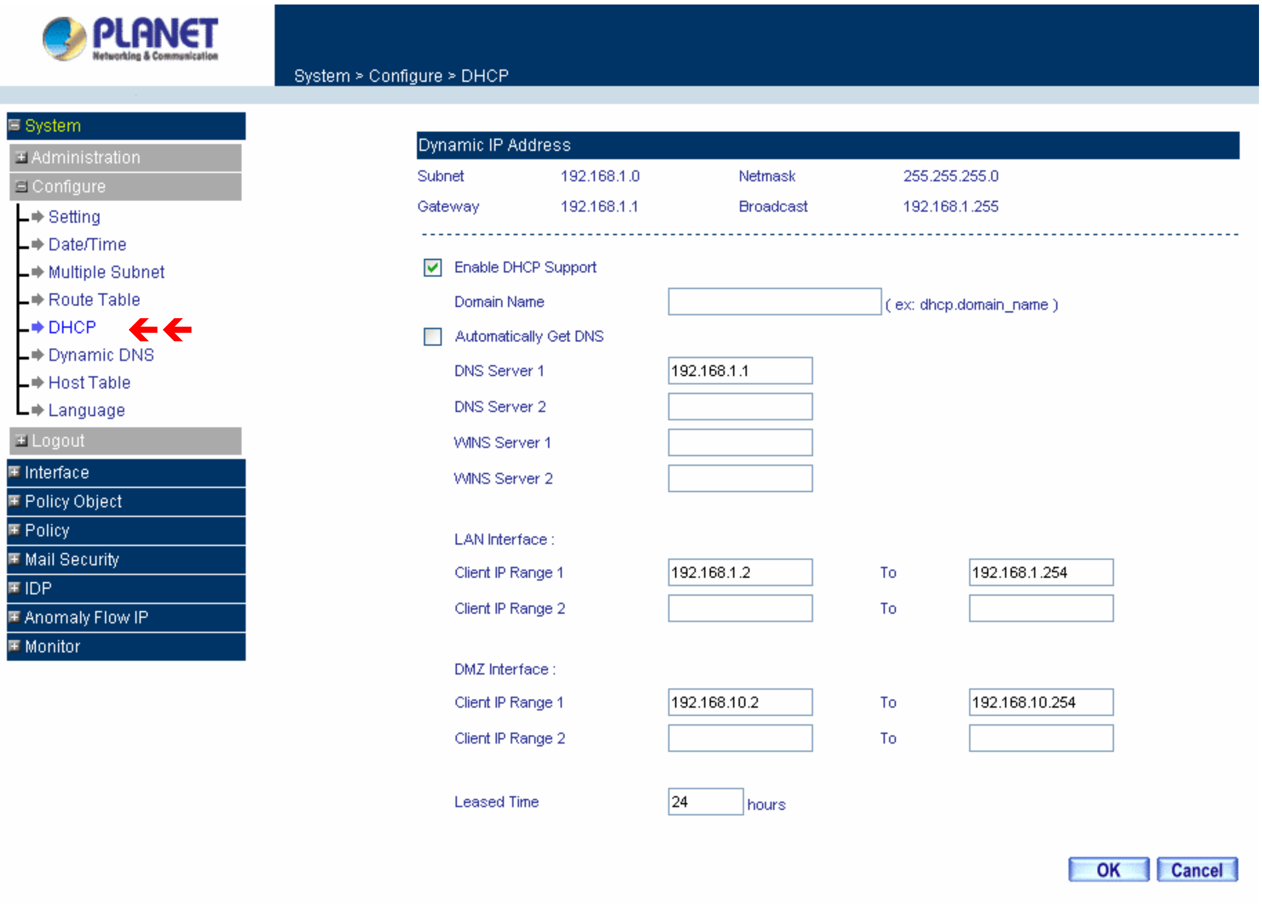
OK Cancel

4.1.8 DHCP

In the section, the Administrator can configure DHCP (Dynamic Host Configuration Protocol) settings for the LAN (LAN) network.

Entering the DHCP window

Click **System** on the left hand side menu bar, then click **DHCP** below the **Configure** menu. The DHCP window appears in which current DHCP settings are shown on the screen.



Dynamic IP Address

Subnet	192.168.1.0	Netmask	255.255.255.0
Gateway	192.168.1.1	Broadcast	192.168.1.255

☑ Enable DHCP Support

Domain Name (ex: dhcp.domain_name)

☐ Automatically Get DNS

DNS Server 1: 192.168.1.1

DNS Server 2:

WINS Server 1:

WINS Server 2:

LAN Interface :

Client IP Range 1: 192.168.1.2 To 192.168.1.254

Client IP Range 2: To

DMZ Interface :

Client IP Range 1: 192.168.10.2 To 192.168.10.254

Client IP Range 2: To

Leased Time: 24 hours

OK Cancel

Dynamic IP Address functions

- **Subnet:** LAN network's subnet
- **Netmask:** LAN network's netmask
- **Gateway:** LAN network's gateway IP address
- **Broadcast:** LAN network's broadcast IP address

Enabling DHCP Support

Step 1. In the Dynamic IP Address window, click **Enable DHCP Support**.

Domain Name: The Administrator may enter the name of the LAN network domain if preferred.

Automatically Get DNS: Check this box to automatically detect DNS server.

DNS Server 1 : Enter the distributed IP address of DNS Server 1.

DNS Server 2 : Enter the distributed IP address of DNS Server 2.

WINS Server 1 : Enter the distributed IP address of WINS Server 1.

WINS Server 2 : Enter the distributed IP address of WINS Server 2.

LAN interface:

Client IP Address Range 1: Enter the starting and the ending IP address dynamically assigning to DHCP clients.

Client IP Address Range 2: Enter the starting and the ending IP address dynamically assigning to DHCP clients. (Optional)

DMZ interface:

Client IP Address Range 1: Enter the starting and the ending IP address dynamically assigning to DHCP clients.

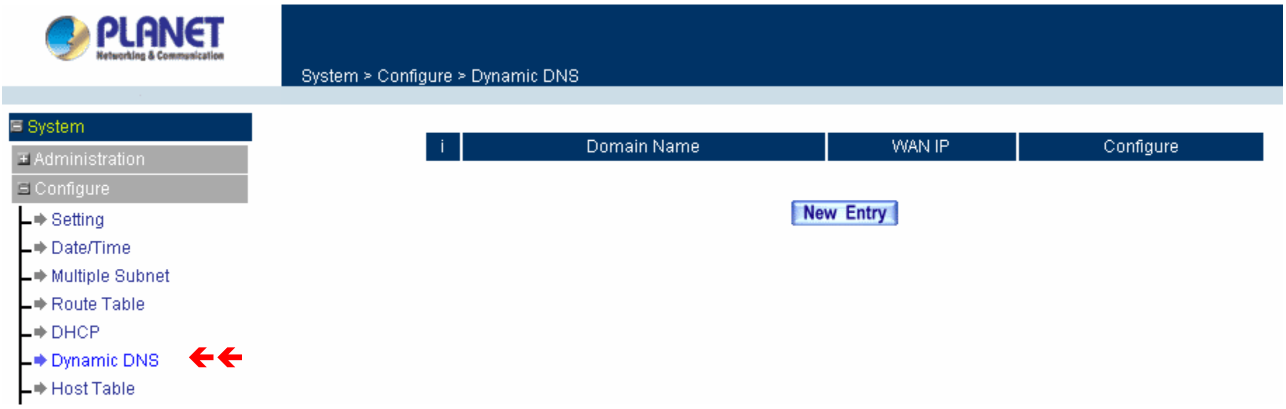
Client IP Address Range 2: Enter the starting and the ending IP address dynamically assigning to DHCP clients. (Optional)

Leased Time: Enter the leased time for DHCP.

Step 2. Click **OK** to enable DHCP support.

4.1.9 Dynamic DNS

The **Dynamic DNS** (require Dynamic DNS Service) allows you to alias a dynamic IP address to a static hostname, allowing your device to be more easily accessed by specific name. When this function is enabled, the IP address in Dynamic DNS Server will be automatically updated with the new IP address provided by ISP.



i	Domain Name	WAN IP	Configure

Click **Dynamic DNS** in the **System** menu to enter Dynamic DNS window.

The icons in Dynamic DNS window:

!: Update Status, 🖥Connecting; ✓Update succeed; ✗Update fail; ⚠Unidentified error.

Domain name: Enter the password provided by ISP.

WAN IP Address: IP address of the WAN port.

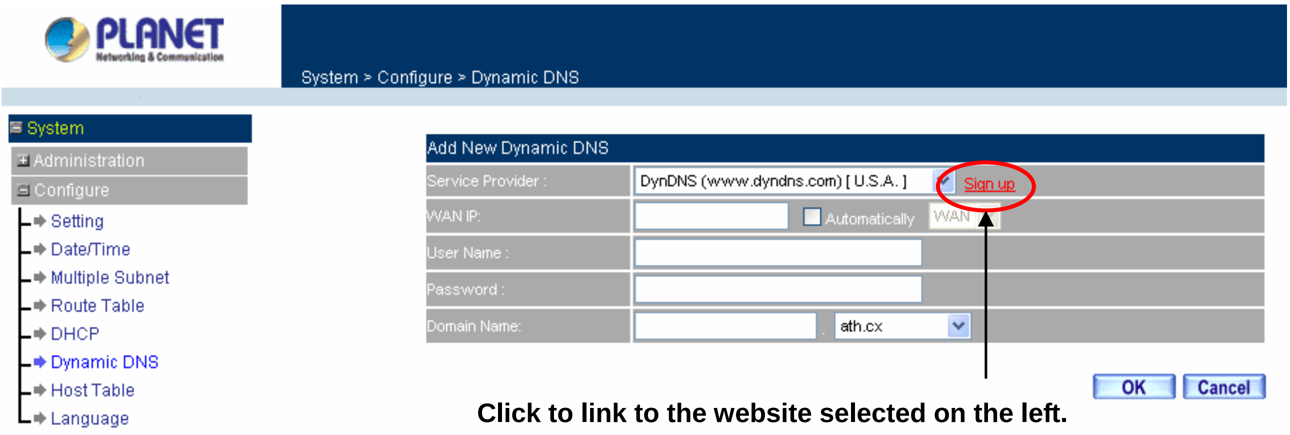
Configure: Modify dynamic DNS settings. Click **Modify** to change the DNS parameters; click Delete to delete the settings.

How to use dynamic DNS:

The Content Security Gateway provides many service providers, users have to register prior to use this function. For the usage regulations, see the providers' websites.

How to register:

Firstly, Click **Dynamic DNS** in the **System** menu to enter Dynamic DNS window, then click **Add** button on the right side of the service providers, click **Sign up**, the service providers' website will appear, please refer to the website for the way of registration.



Service Provider :	DynDNS (www.dyndns.com) [U.S.A.]
WAN IP:	□ Automatically WAN
User Name :	
Password :	
Domain Name:	. ath.cx

Click to link to the website selected on the left.

Add Dynamic DNS settings

Step 1. Click **Add** button.

Step 2. Click the information in the column of the new window.

Service providers: Select service providers.

Sign up: to the service providers' website.

WAN IP Address: IP Address of the WAN port.

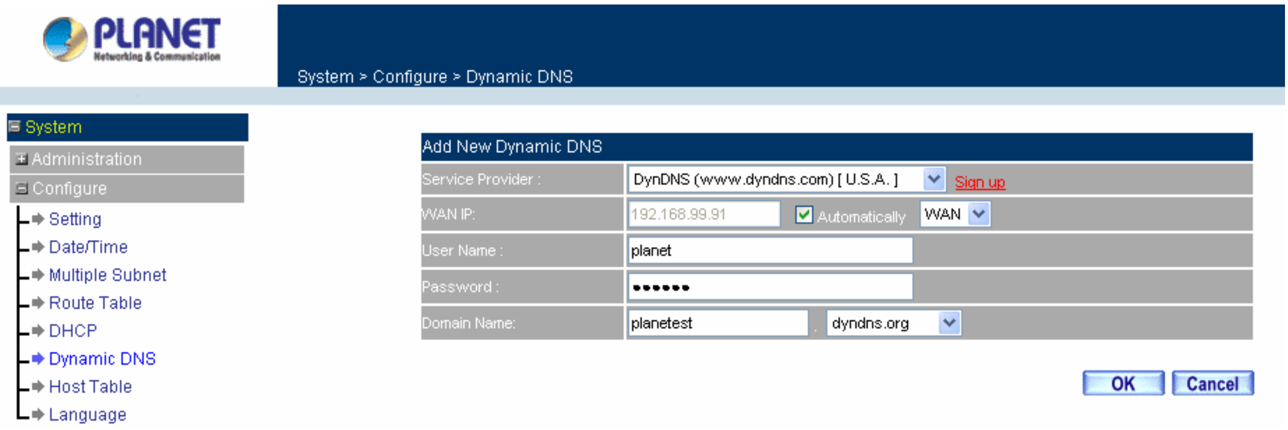
□ **Automatically** : Check to automatically fill in the WAN IP.。

User Name: Enter the registered user name.

Password: Enter the password provided by ISP (Internet Service Provider).

Domain name: Your host domain name provided by ISP.

Click **OK** to add dynamic DNS or click **Cancel** to discard changes.



Add New Dynamic DNS

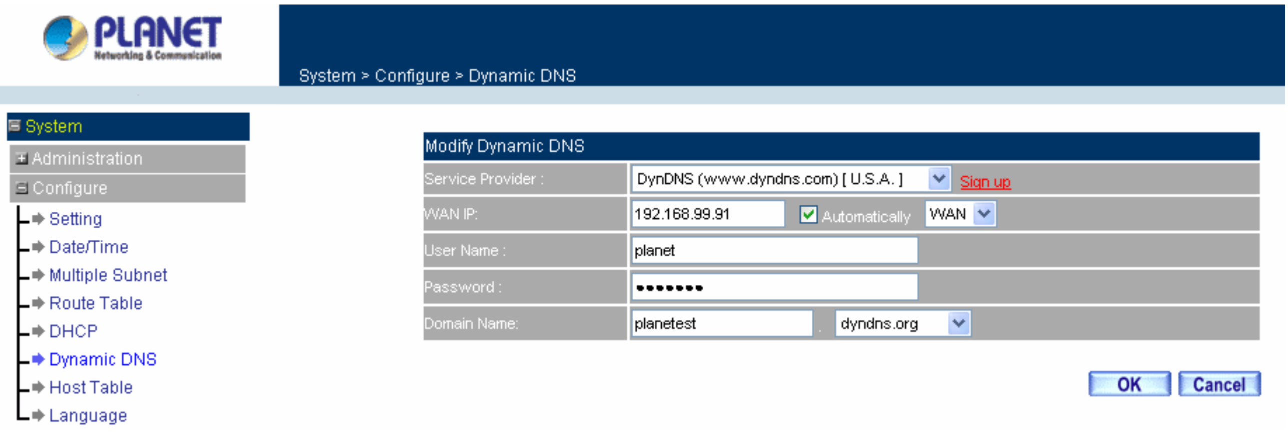
Service Provider :	DynDNS (www.dyndns.com) [U.S.A.] Sign up
WAN IP:	192.168.99.91 ☑ Automatically WAN
User Name :	planet
Password :	••••••
Domain Name:	planetest . dyndns.org

Modify dynamic DNS

Step 1. Find the item you want to change and click **Modify**.

Step 2. Enter the new information in the Modify Dynamic DNS window.

Click **OK** to change the settings or click **Cancel** to discard changes.



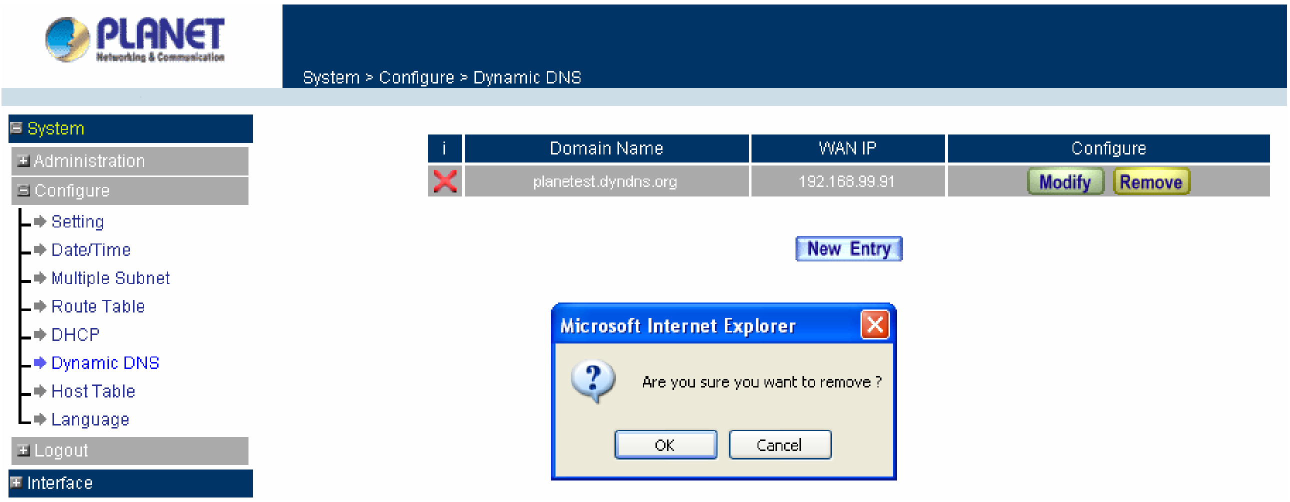
Modify Dynamic DNS

Service Provider :	DynDNS (www.dyndns.com) [U.S.A.] Sign up
WAN IP:	192.168.99.91 ☑ Automatically WAN
User Name :	planet
Password :	•••••••
Domain Name:	planetest . dyndns.org

Remove Dynamic DNS

Step 1. Find the item you want to change and click **Remove**.

Step 2. A confirmation pop-up box will appear, click OK to delete the settings or click Cancel to discard changes.



i	Domain Name	WAN IP	Configure
☒	planetest.dyndns.org	192.168.99.91	Modify Remove

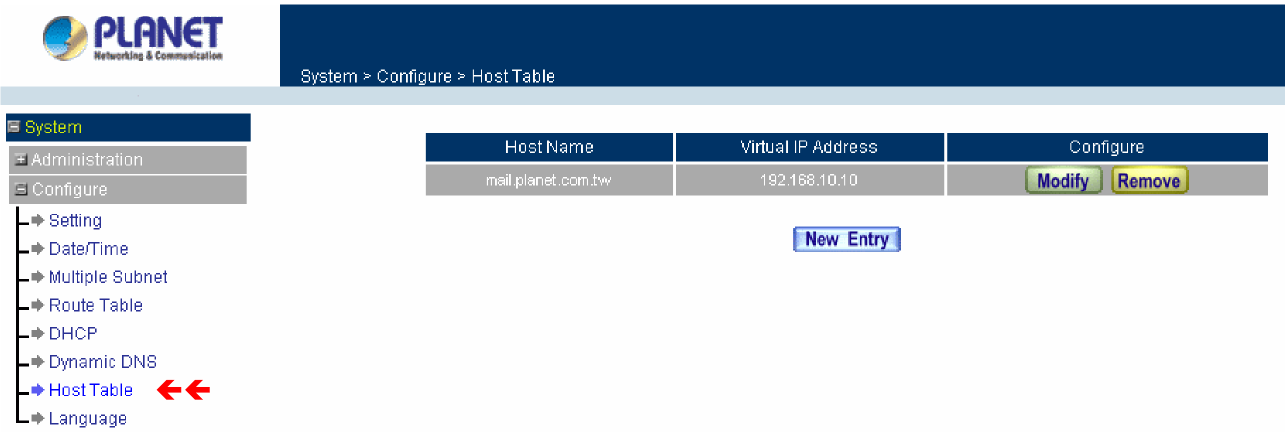
Are you sure you want to remove ?

4.1.10 Host Table

The Content Security Gateway's Administrator may use the Host Table function to make the Content Security Gateway act as a DNS Server for the LAN and DMZ network. All DNS requests to a specific Domain Name will be routed to the Content Security Gateway's IP address. For example, let's say an organization has their mail server (i.e., mail.planet.com.tw) in the DMZ network (i.e. 192.168.10.10). The outside Internet world may access the mail server of the organization easily by its domain name, providing that the Administrator has set up Virtual Server or Mapped IP settings correctly. However, for the users in the LAN network, their WAN DNS server will assign them a public IP address for the mail server. So for the LAN network to access the mail server (mail.planet.com.tw), they would have to go out to the Internet, then come back through the Content Security Gateway to access the mail server. Essentially, the LAN network is accessing the mail server by a real public IP address, while the mail server serves their request by a NAT address and not a real one.
This odd situation occurs when there are servers in the DMZ network and they are bound to real IP addresses. To avoid this, set up Host Table so all the LAN network computers will use the Content Security Gateway as a DNS server, which acts as the DNS proxy.

If you want to use the Host Table function of the device, the end user's main DNS server IP address should be the same IP Address as the device.

Click on **System** in the menu bar, then click on **Host Table** below the **Configure** menu. The Host Table window will appear.



System > Configure > Host Table

Host Name	Virtual IP Address	Configure
mail.planet.com.tw	192.168.10.10	Modify Remove

Below is the information needed for setting up the **Host Table**:

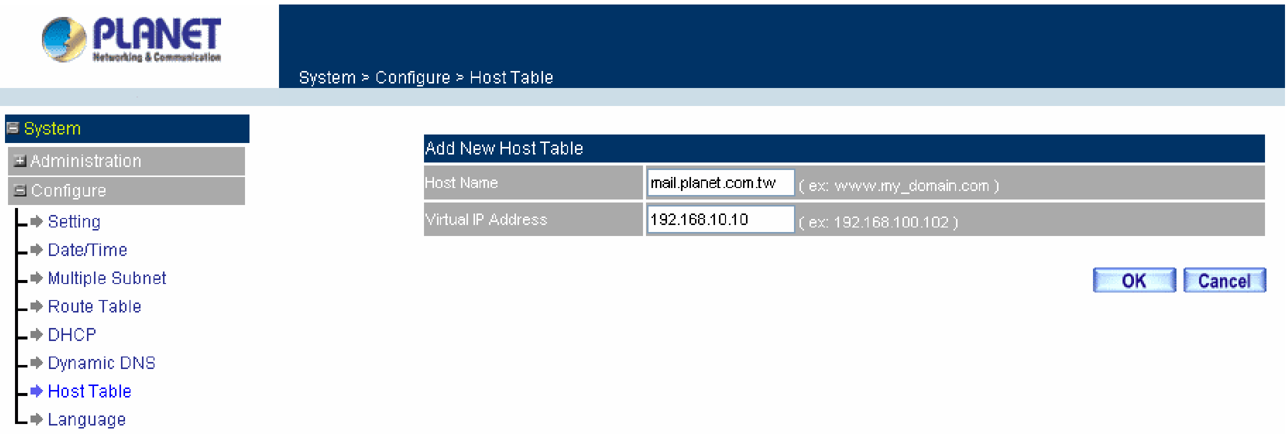
- **Host Name:** The domain name of the server
- **Virtual IP Address:** The virtual IP address respective to Host Table
- **Configure:** modify or remove each Host Table policy

Adding a new Host Table

Step 1: Click on the **New Entry** button and the **Add New Host Table** window will appear.

Step 2: Fill in the appropriate settings for the domain name and virtual IP address.

Step 3: Click **OK** to save the policy or **Cancel** to cancel.



System > Configure > Host Table

Add New Host Table

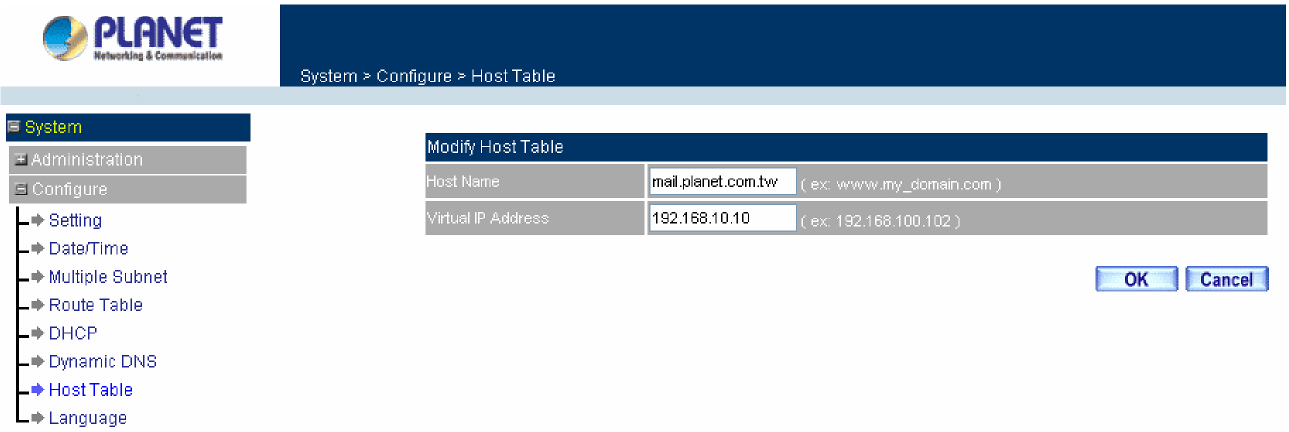
Host Name	mail.planet.com.tw	(ex: www.my_domain.com)
Virtual IP Address	192.168.10.10	(ex: 192.168.100.102)

Modifying a Host Table

Step 1: In the **Host Table** window, find the policy to be modified and click the corresponding **Modify** option in the **Configure** field.

Step 2: Make the necessary changes needed.

Step 3: Click **OK** to save changes or click on **Cancel** to cancel modifications.



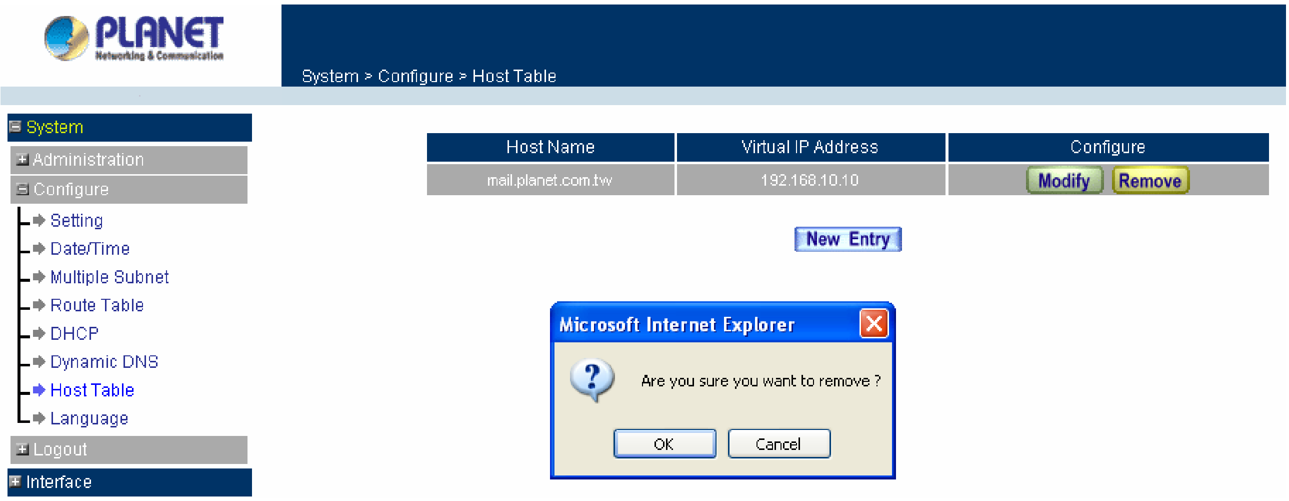
Modify Host Table

Host Name	mail.planet.com.tw	(ex: www.my_domain.com)
Virtual IP Address	192.168.10.10	(ex: 192.168.100.102)

Removing a Host Table

Step 1: In the **Host Table** window, find the policy to be removed and click the corresponding **Remove** option in the **Configure** field.

Step 2: A confirmation pop-up box will appear, click **OK** to remove the Host Table or click **Cancel**.



Host Name	Virtual IP Address	Configure
mail.planet.com.tw	192.168.10.10	Modify Remove

Are you sure you want to remove ?

4.1.11 Language

Administrator can configure the Content Security Gateway to select the Language version.

Step 1. Select the Language version (**English Version, Traditional Chinese Version** or **Simplified Chinese Version**).

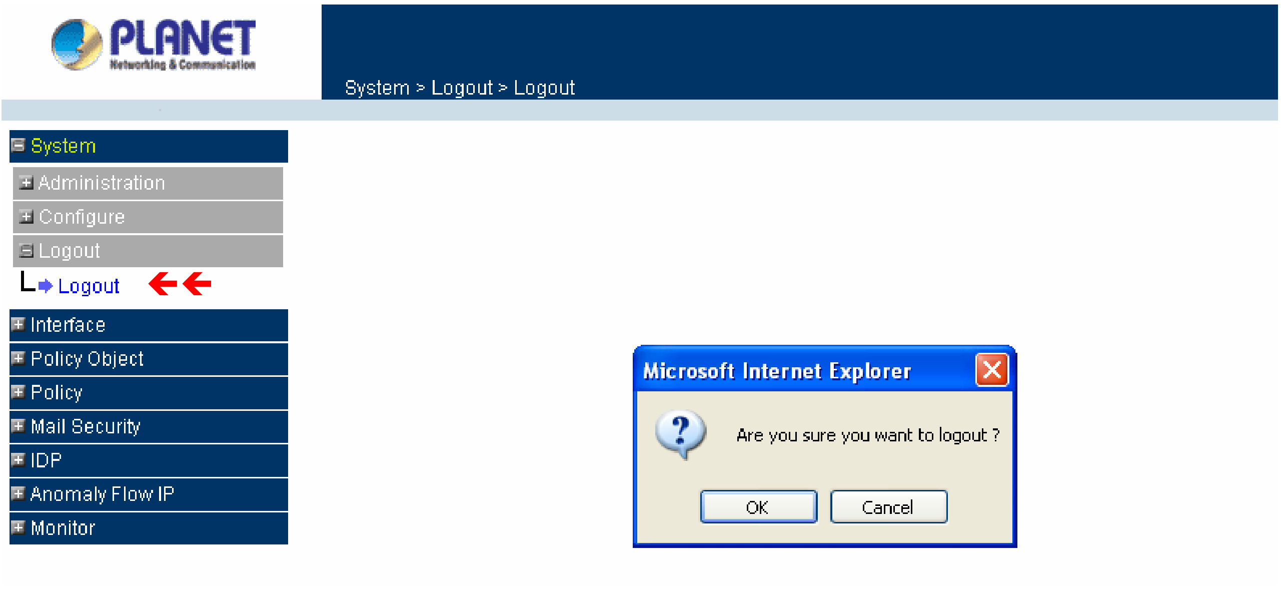
Step 2. Click **[OK]** to set the Language version or click **Cancel** to discard changes.

4.1.12 Logout

Step 1. Select this option to the device's **Logout** the Content Security Gateway. This function protects your system while you are away.

Step 2. Click Logout the Content Security Gateway.

Step 3. Click **OK** to logout or click **Cancel** to discard the change.



Are you sure you want to logout ?

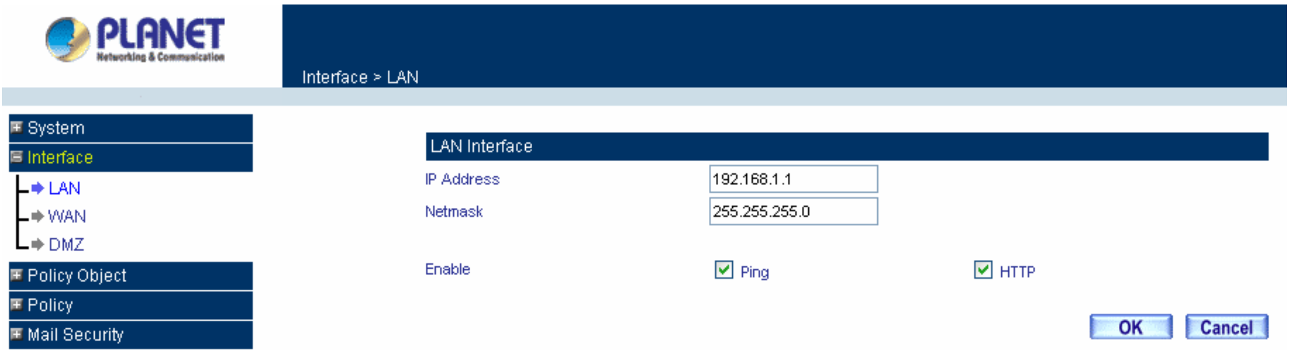
4.2 Interface

In this section, the **Administrator** can set up the IP addresses for the office network. The Administrator may configure the IP addresses of the LAN network, the WAN network, and the DMZ network. The netmask and gateway IP addresses are also configured in this section.

4.2.1 LAN

Entering the Interface menu:

Click on **Interface** in the left menu bar. Then click on **LAN** below it. The current settings of the interface addresses will appear on the screen.



IP Address: 192.168.1.1
Netmask: 255.255.255.0
Enable: ☑ Ping ☑ HTTP

Configuring the Interface Settings

Using the LAN **Interface**, the Administrator sets up the LAN network. The LAN network will use a private IP scheme. The private IP network will not be routable on the Internet.

IP Address: The private IP address of the Content Security Gateway's LAN network is the IP address of the LAN port of the device. The default IP address is 192.168.1.1. If the new LAN IP Address is not 192.168.1.1, the Administrator needs to set the IP Address on the computer to be on the same subnet as the Content Security Gateway and restart the System to make the new IP address effective. For example, if the Content Security Gateway's new LAN IP Address is 172.16.0.1, then enter the new LAN IP Address 172.16.0.1 in the URL field of browser to connect to Content Security Gateway.

NetMask: This is the subnet mask of the LAN network. The default netmask of the device is 255.255.255.0.

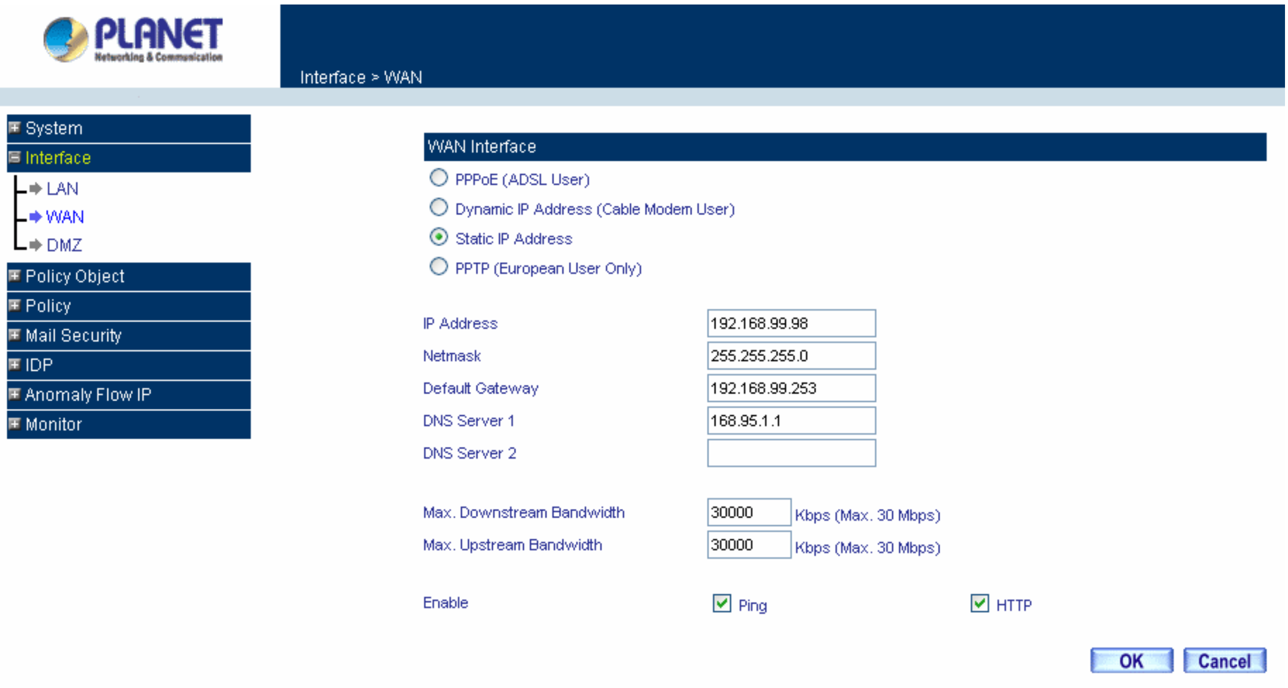
Ping: Select this to allow the LAN network to ping the IP Address of the Content Security Gateway. If set to enable, the device will respond to ping packets from the LAN network.

HTTP: Select this to allow the device WEBUI to be accessed from the LAN network.

4.2.2 WAN

Entering the Interface menu

Click on **Interface** in the left menu bar. Then click on **WAN** below it. The current settings of the interface addresses will appear on the screen.



WAN Interface

○ PPPoE (ADSL User)
○ Dynamic IP Address (Cable Modem User)
● Static IP Address
○ PPTP (European User Only)

IP Address	192.168.99.98
Netmask	255.255.255.0
Default Gateway	192.168.99.253
DNS Server 1	168.95.1.1
DNS Server 2	
Max. Downstream Bandwidth	30000 Kbps (Max. 30 Mbps)
Max. Upstream Bandwidth	30000 Kbps (Max. 30 Mbps)
Enable	☑ Ping ☑ HTTP

WAN Interface

Using the WAN **Interface**, the Administrator can sets up the **WAN** network. These IP addresses are real public IP Addresses, and are routable on the Internet.

For PPPoE (ADSL User): This option is for PPPoE users who are required to enter a username and password in order to connect, such as ADSL users.

Current Status: Displays the current line status of the PPPoE connection.

IP Address: Displays the IP address of the PPPoE connection

Username: Enter the PPPoE username provided by the ISP.

Password: Enter the PPPoE password provided by the ISP.

IP Address provided by ISP:

Dynamic: Select this if the IP address is automatically assigned by the ISP.

Fixed: Select this if you were given a static IP address. Enter the IP address that is given to you by your ISP.

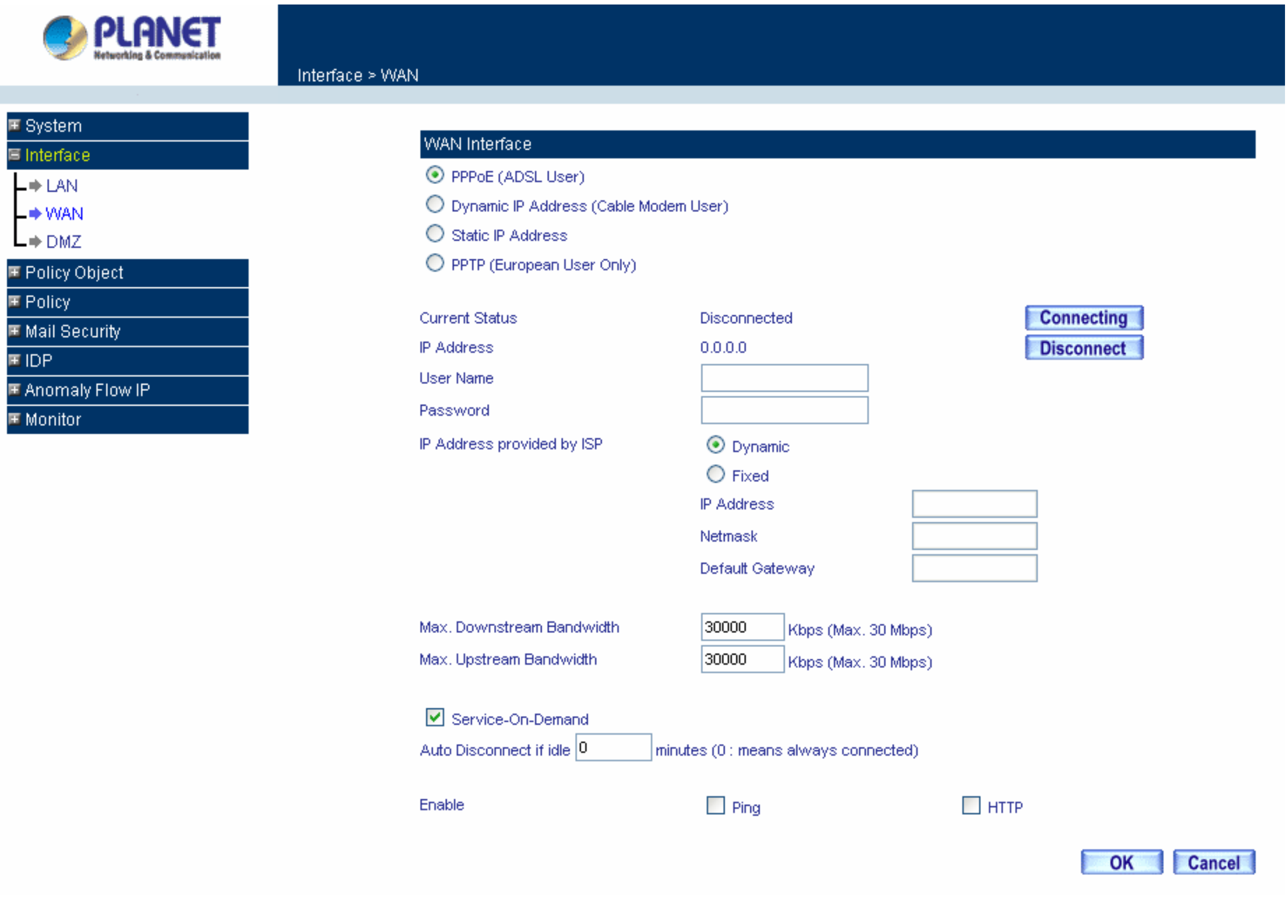
Max. Upstream/Downstream Bandwidth: The bandwidth provided by ISP.

Service-On-Demand:

Auto Disconnect: The PPPoE connection will automatically disconnect after a length of idle time (no activities). Enter in the amount of idle minutes before disconnection. Enter '0' if you do not want the PPPoE connection to disconnect at all.

Ping: Select this to allow the WAN network to ping the IP address of the Content Security Gateway. This will allow people from the Internet to be able to ping the Content Security Gateway. If it sets to enable, the device will respond to echo request packets from the WAN network.

HTTP: Select this to allow the device WebUI to be accessed from the WAN network. This will allow the WebUI to be configured from a user on the Internet. Keep in mind that the device always requires a username and password to enter the WebUI.



● PPPoE (ADSL User)
○ Dynamic IP Address (Cable Modem User)
○ Static IP Address
○ PPTP (European User Only)

Current Status: Disconnected
IP Address: 0.0.0.0
User Name:
Password:
IP Address provided by ISP: ● Dynamic ○ Fixed
IP Address:
Netmask:
Default Gateway:

Max. Downstream Bandwidth: 30000 Kbps (Max. 30 Mbps)
Max. Upstream Bandwidth: 30000 Kbps (Max. 30 Mbps)

☑ Service-On-Demand
Auto Disconnect if idle 0 minutes (0 : means always connected)

Enable □ Ping □ HTTP

For Dynamic IP Address (Cable Modem User): This option is for users who are automatically assigned an IP address by their ISP, such as cable modem users. The following fields apply:

IP Address: The dynamic IP address obtained by the Content Security Gateway from the ISP will be displayed here. This is the IP address of the WAN port of the device.

MAC Address: This is the MAC Address of the device.

Hostname: This will be the name assign to the device. Some cable modem ISP assign a specific hostname in order to connect to their network. Please enter the hostname here. If not required by your ISP, you do not have to enter a hostname.

Domain Name: You can specify your own domain name or leave it blank.

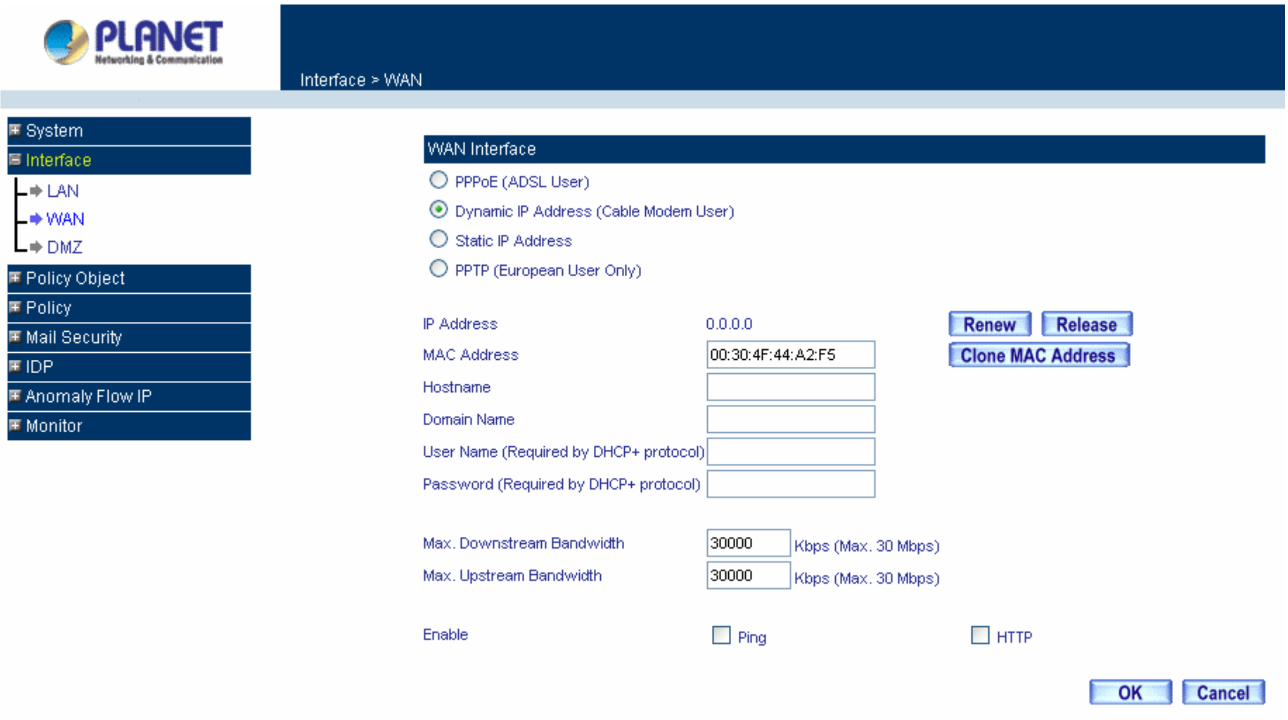
User Name: The user name is provided by ISP.

Password: The password is provided by ISP.

Max. Upstream/Downstream Bandwidth: The bandwidth provided by ISP.

Ping: Select this to allow the WAN network to ping the IP Address of the Content Security Gateway. This will allow people from the Internet to be able to ping the Content Security Gateway. If set to enable, the device will respond to echo request packets from the WAN network.

HTTP: Select this to allow the device WEBUI to be accessed from the WAN network. This will allow the WebUI to be configured from a user on the Internet. Keep in mind that the device always requires an username and password to enter the WebUI.



WAN Interface

○ PPPoE (ADSL User)
● Dynamic IP Address (Cable Modem User)
○ Static IP Address
○ PPTP (European User Only)

IP Address	0.0.0.0
MAC Address	00:30:4F:44:A2:F5
Hostname	
Domain Name	
User Name (Required by DHCP+ protocol)	
Password (Required by DHCP+ protocol)	
Max. Downstream Bandwidth	30000 Kbps (Max. 30 Mbps)
Max. Upstream Bandwidth	30000 Kbps (Max. 30 Mbps)
Enable	□ Ping □ HTTP

<u>**For Static IP Address:**</u> This option is for users who are assigned a static IP address from their ISP. Your ISP will provide all the information needed for this section such as IP address, Netmask, Gateway, and DNS. Use this option also if you have more than one public IP Address assigned to you.

IP Address: Enter the static IP address assigned to you by your ISP. This will be the public IP address of the WAN port of the device.

Netmask: This will be the subnet mask of the WAN network. (i.e. 255.255.255.0)

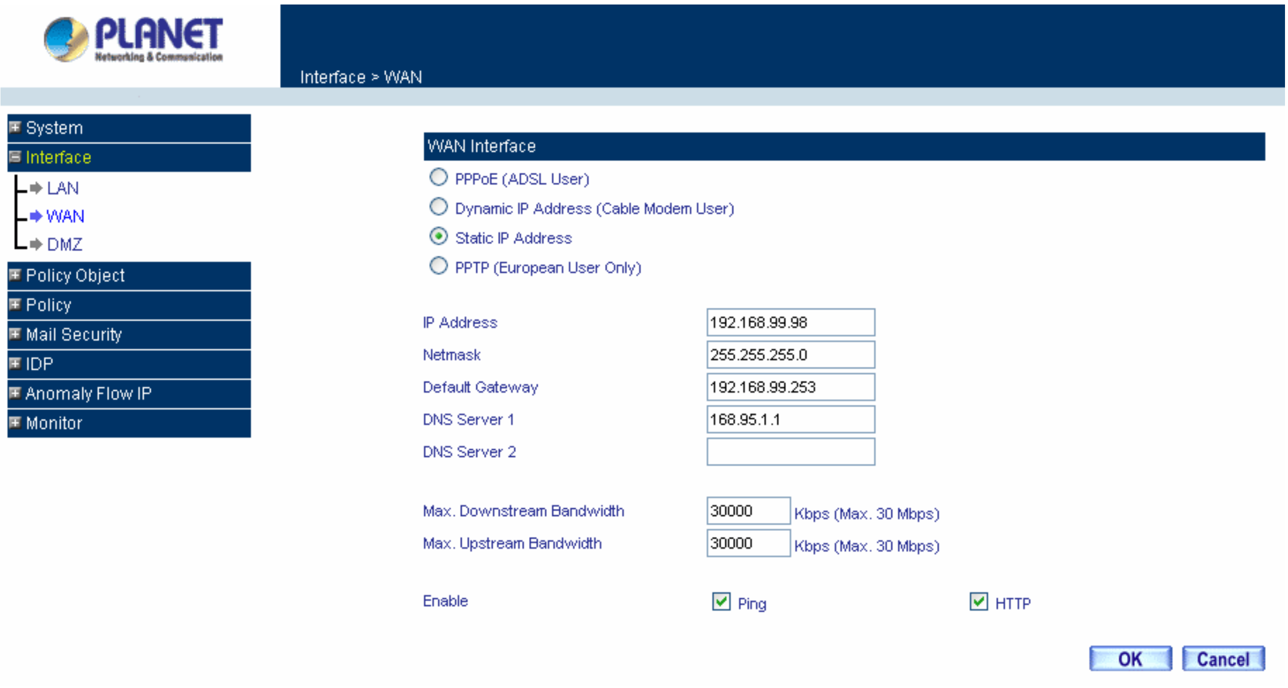
Default Gateway: This will be the Gateway IP address.

Domain Name Server (DNS): This is the IP address of the DNS server.

Max. Upstream/Downstream Bandwidth: The bandwidth provided by ISP.

Ping: Select this to allow the WAN network to ping the IP Address of the Content Security Gateway. This will allow people from the Internet to be able to ping the Content Security Gateway. If set to enable, the device will respond to echo request packets from the WAN network.

HTTP: Select this to allow the device WebUI to be accessed from the WAN network. This will allow the WebUI to be configured from a user on the Internet. Keep in mind that the device always requires a username and password to enter the WebUI.



WAN Interface

○ PPPoE (ADSL User)
○ Dynamic IP Address (Cable Modem User)
● Static IP Address
○ PPTP (European User Only)

IP Address	192.168.99.98
Netmask	255.255.255.0
Default Gateway	192.168.99.253
DNS Server 1	168.95.1.1
DNS Server 2	
Max. Downstream Bandwidth	30000 Kbps (Max. 30 Mbps)
Max. Upstream Bandwidth	30000 Kbps (Max. 30 Mbps)
Enable	☑ Ping ☑ HTTP

__For PPTP (European User Only):__ This is mainly used in Europe. You need to know the PPTP Server address as well as your name and password.

User Name: The user name is provided by ISP.

Password: The password is provided by ISP.

IP Address: Enter the static IP address assigned to you by your ISP, or obtain an IP address automatically from ISP.

PPTP Gateway: Enter the PPTP server IP address assigned to you by your ISP.

Connect ID: This is the ID given by ISP. This is optional.

Max. Upstream/Downstream Bandwidth: The bandwidth provided by ISP.

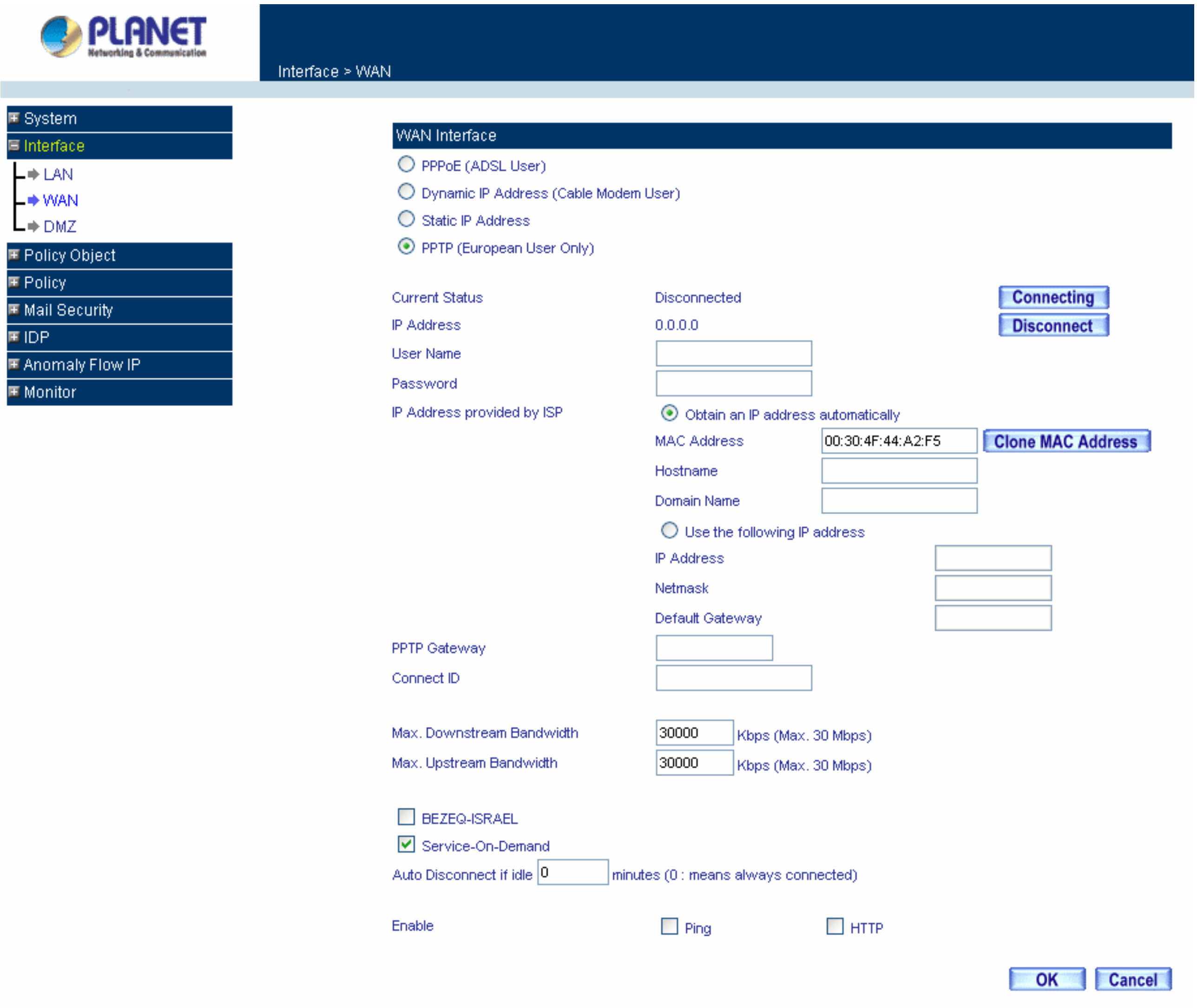
BEZEQ-ISRAEL: Select this item if you are using the service provided by BEZEQ in Israel.

Service-On-Demand:

The PPPoE connection will automatically disconnect after a length of idle time (no activities). Enter in the amount of idle minutes before disconnection. Enter '0' if you do not want the PPPoE connection to disconnect at all.

Ping: Select this to allow the WAN network to ping the IP address of the Content Security Gateway. This will allow people from the Internet to be able to ping the Content Security Gateway. If set to enable, the device will respond to echo request packets from the WAN network.

HTTP: Select this to allow the device WEBUI to be accessed from the WAN network. This will allow the WebUI to be configured from a user on the Internet. Keep in mind that the device always requires a username and password to enter the WebUI.



WAN Interface

○ PPPoE (ADSL User)
○ Dynamic IP Address (Cable Modem User)
○ Static IP Address
● PPTP (European User Only)

Current Status: Disconnected
IP Address: 0.0.0.0
User Name:
Password:
IP Address provided by ISP: ● Obtain an IP address automatically
MAC Address: 00:30:4F:44:A2:F5
Hostname:
Domain Name:
○ Use the following IP address
IP Address:
Netmask:
Default Gateway:
PPTP Gateway:
Connect ID:

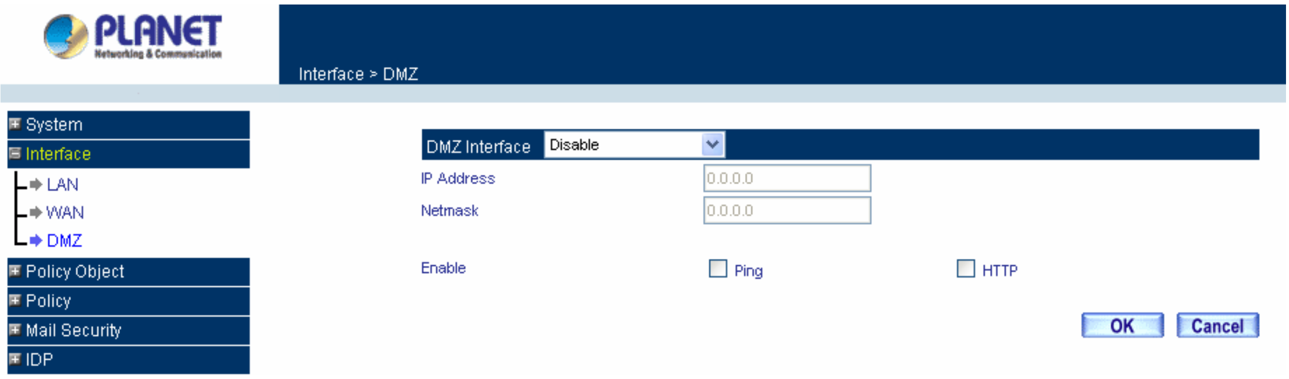
Max. Downstream Bandwidth: 30000 Kbps (Max. 30 Mbps)
Max. Upstream Bandwidth: 30000 Kbps (Max. 30 Mbps)

□ BEZEQ-ISRAEL
☑ Service-On-Demand
Auto Disconnect if idle 0 minutes (0 : means always connected)

Enable □ Ping □ HTTP

4.2.3 DMZ

The Administrator uses the **DMZ Interface** to set up the DMZ network. The DMZ network consists of server computers such as FTP, SMTP, and HTTP (web). These server computers are put in the DMZ network so they can be isolated from the LAN (LAN) network traffic. Broadcast messages from the LAN network will not cross over to the DMZ network to cause congestions and slow down these servers. This allows the server computers to work efficiently without any slowdowns.



DMZ Interface: Disable

IP Address: 0.0.0.0

Netmask: 0.0.0.0

Enable: □ Ping □ HTTP

DMZ Interface: Display DMZ NAT Mode /DMZ TRANSPARENT Mode functions of DMZ to show if they are enabled or disabled.

IP Address: The private IP address of the Content Security Gateway's DMZ interface. This will be the IP address of the DMZ port. If it is in NAT mode, the IP address the Administrator chooses will be a private IP address and cannot use the same network as the WAN or LAN network.

NetMask: This will be the subnet mask of the DMZ network.

Ping: Select this to allow the DMZ network to ping the IP Address of the Content Security Gateway. This will allow people from the Internet to be able to ping the Content Security Gateway. If set to enable, the device will respond to echo request packets from the DMZ network.

HTTP: Select this to allow the device WebUI to be accessed from the DMZ network. This will allow the WebUI to be configured from a user on the Internet. Keep in mind that the device always requires a username and password to enter the WebUI.

4.3 Policy Object

The Policy Object is the pre-setting item for Policy editing. The administrator can configure all necessary items here before he wants to configure Content Security Gateway Policy. The contents include **Address**, **Service, Schedule**, **QoS**, **Authentication**, **Content Blocking**, **Virtual server** and **VPN**.

4.3.1 Address

The Content Security Gateway allows the Administrator to set addresses of the LAN network, LAN network group, WAN network, WAN group, DMZ network and DMZ group.

What is the Address Table?

An IP address in the Address Table can be an address of a computer or a sub network. The Administrator can assign an easily recognized name to an IP address. Based on the network it belongs to, an IP address can be an LAN IP address, WAN IP address and DMZ IP address. If the Administrator needs to create a control policy for packets of different IP addresses, he can first add a new group in the **LAN Network Group** or the **WAN Network Group** and assign those IP addresses into the newly created group. Using group addresses can greatly simplify the process of building control policies.

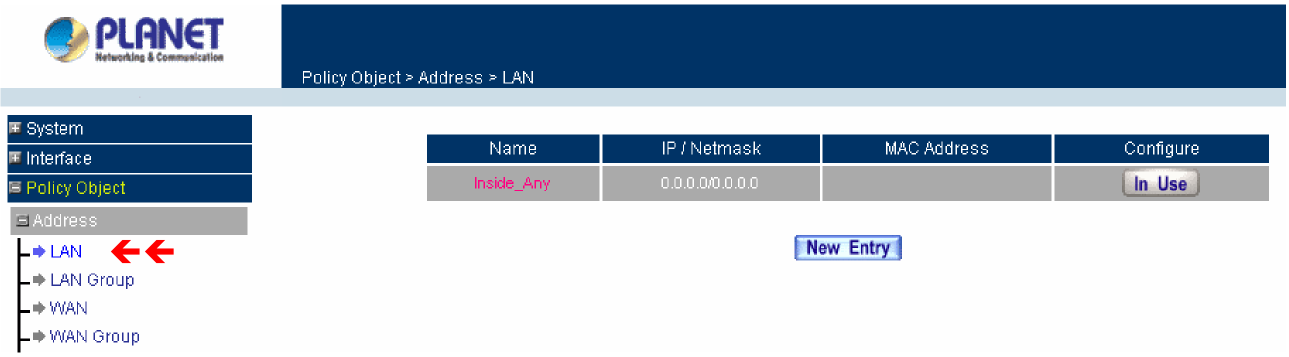
How to use Address Table

With easily recognized names of IP addresses and names of address groups shown in the address table, the Administrator can use these names as the source address or destination address of control policies. The address table should be built before creating control policies, so that the Administrator can pick the names of correct IP addresses from the address table when setting up control policies.

4.3.1.1 LAN

Entering the LAN window

Step 1. Click LAN under the **Address** menu to enter the LAN window. The current setting information such as the name of the LAN network, IP and Netmask addresses will show on the screen.



Name	IP / Netmask	MAC Address	Configure
Inside_Any	0.0.0.0/0.0.0.0		In Use

Definition

Name: Name of LAN network address.

IP / Netmask: IP address and subnet mask of LAN network

MAC Address: MAC address corresponded with LAN IP address.

Configure: You can configure the settings in LAN network. Click **Modify** to change the parameters in LAN network. Click **Remove** to delete the settings.

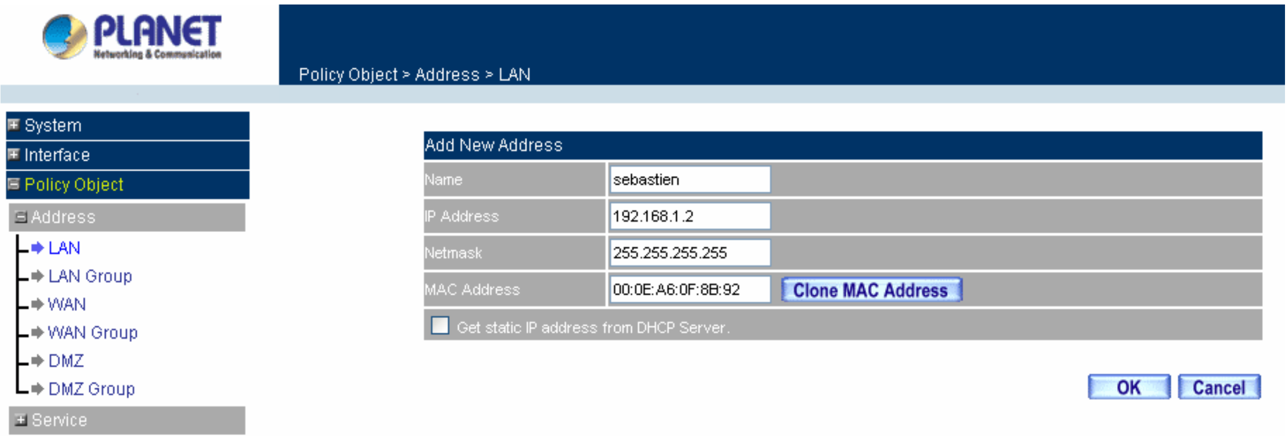
In the **LAN** window, if one of the members has been added to **Policy** or **LAN Group**, the **Configure** column will show the message – **In Use**. In this case, you are not allowed to modify or remove the setting.

Adding a new LAN Address

Step 1. In the LAN window**,** click the **New Entry** button.

Step 2. In the **Add New Address** window, enter the settings of a new LAN network address.

Step 3. Click **OK** to add the specified LAN network or click **Cancel** to cancel the changes.



Add New Address

Name	sebastien
IP Address	192.168.1.2
Netmask	255.255.255.255
MAC Address	00:0E:A6:0F:8B:92

□ Get static IP address from DHCP Server.

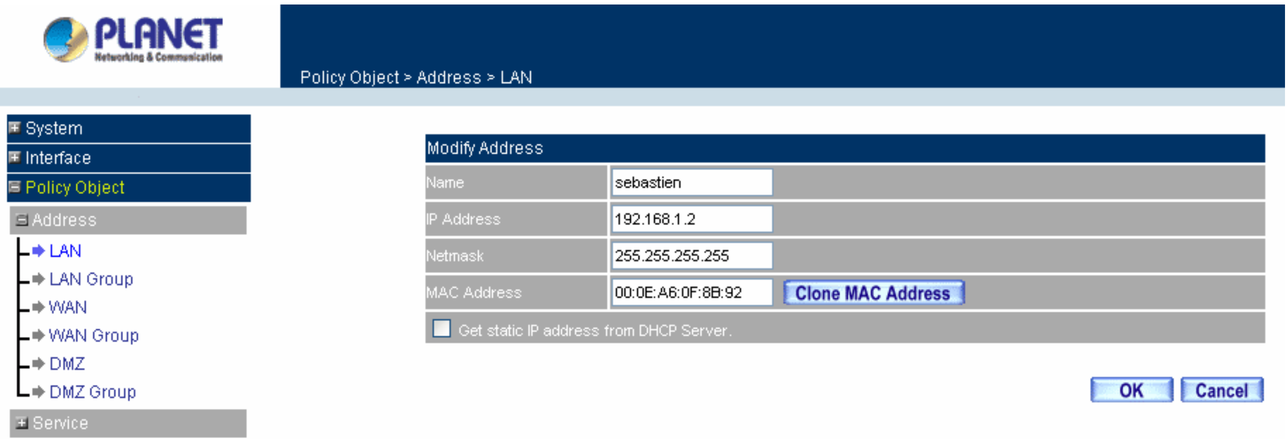
If you want to enable **Get Static IP address from DHCP Server** function, enter the MAC Address then check the **Get Static IP address from DHCP Server**.

Modifying an LAN Address

Step 1. In the LAN window, locate the name of the network to be modified. Click the **Modify** option in its corresponding **Configure** field. The **Modify Address** window appears on the screen immediately.

Step 2. In the **Modify Address** window, fill in the new addresses.

Step 3. Click **OK** to save changes or click **Cancel** to discard changes.



Modify Address

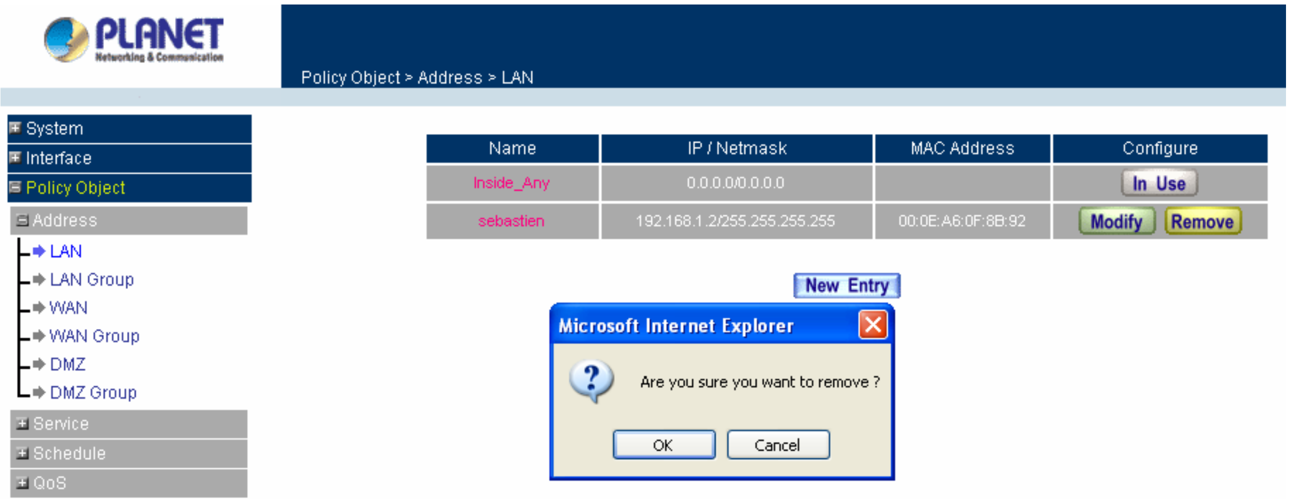
Name	sebastien
IP Address	192.168.1.2
Netmask	255.255.255.255
MAC Address	00:0E:A6:0F:8B:92

□ Get static IP address from DHCP Server.

Removing a LAN Address

Step 1. In the LAN window, locate the name of the network to be removed. Click the **Remove** option in its corresponding **Configure** field.

Step 2. In the **Remove** confirmation pop-up box, click **OK** to remove the address or click **Cancel** to discard changes.



Name	IP / Netmask	MAC Address	Configure
Inside_Any	0.0.0.0/0.0.0.0		In Use
sebastien	192.168.1.2/255.255.255.255	00:0E:A6:0F:8B:92	Modify Remove

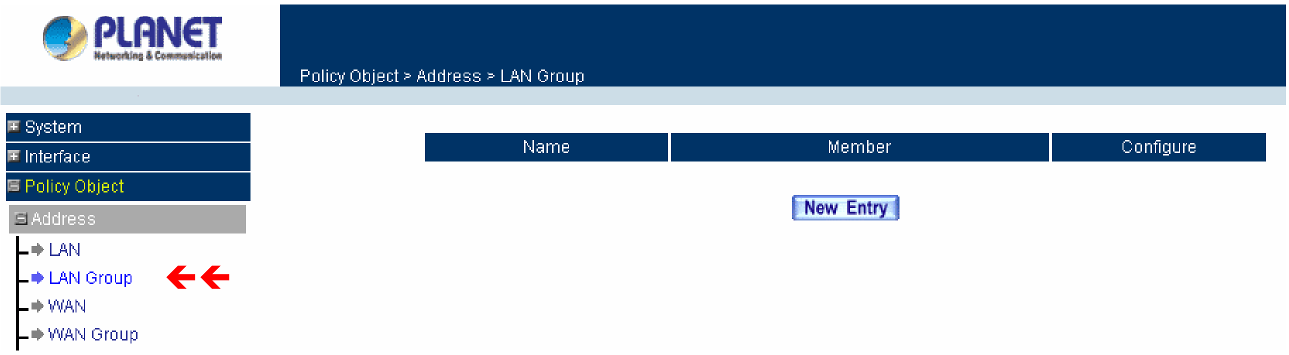
Are you sure you want to remove ?

4.3.1.2 LAN Group

Entering the LAN Group window

The LAN Addresses may be combined together to become a group.

Step 1. Click LAN **Group** under the **Address** menu to enter the LAN Group window. The current setting information for the LAN network group appears on the screen.



Name	Member	Configure

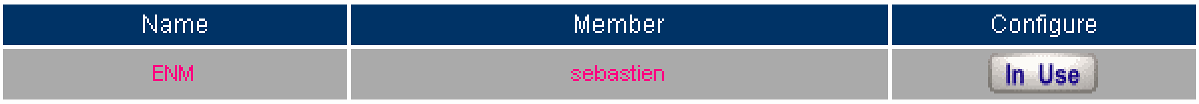
Definitions

Name: Name of the LAN group.

Member: Members of the group.

Configure: Configure the settings of LAN group. Click **Modify** to change the settings of LAN group. Click **Remove** to delete the group.

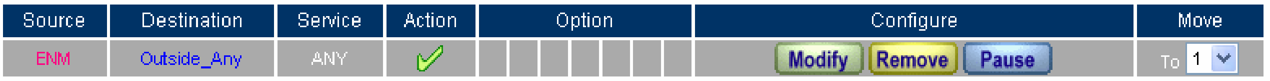
In the **LAN Group** window, if one of the LAN Group has been added to **Policy**, the **Configure** column will show the message – **In Use**. In this case, you are not allowed to modify or remove the LAN group.



Name	Member	Configure
ENM	sebastien	In Use

You have to delete or pause the Group in **Policy** window, and then you are allowed to configure the LAN

Group.



Source	Destination	Service	Action	Option	Configure	Move
ENM	Outside_Any	ANY	✓		Modify Remove Pause	To 1

Adding a LAN Group

Step 1. In the LAN **Group** window, click the **New Entry** button to enter the **Add New Address Group** window.

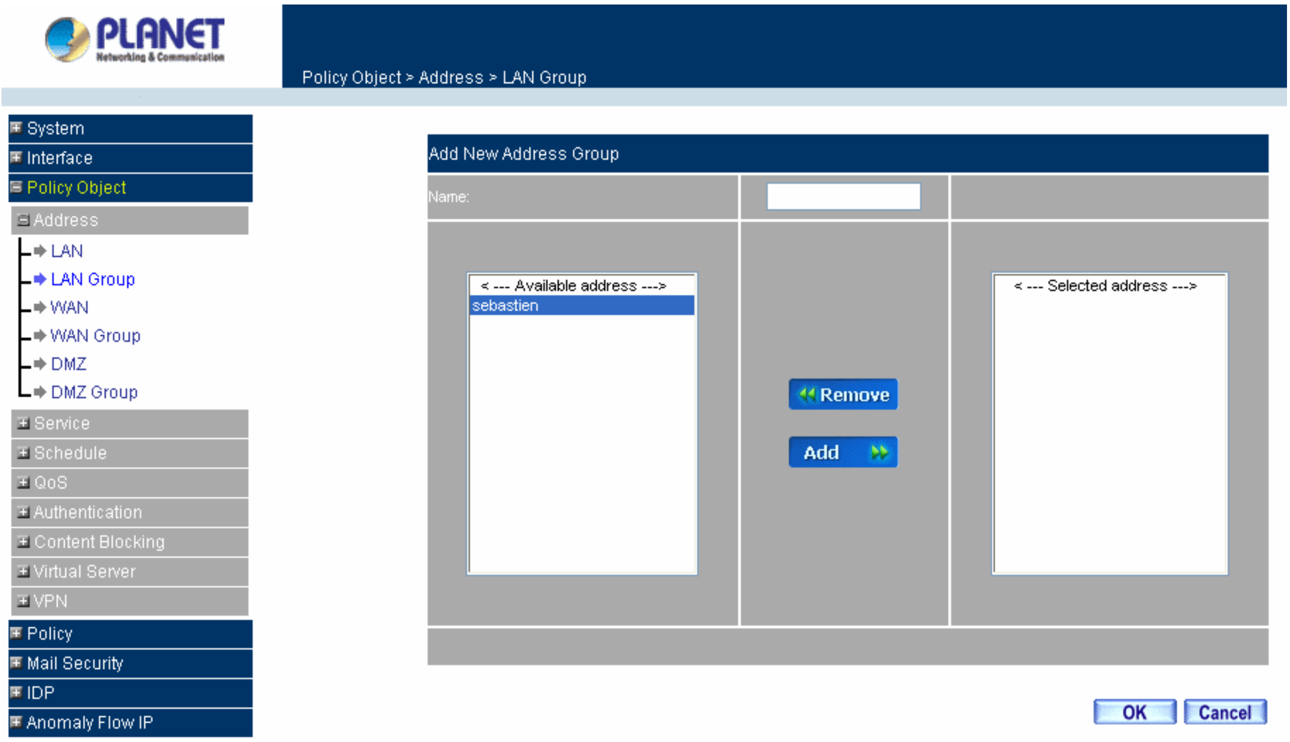
Step 2. In the Add New Address Group window:

- **Available address:** list the names of all the members of the LAN network.
- **Selected address:** list the names to be assigned to the new group.
- **Name:** enter the name of the new group in the open field.

Step 3. **Add members:** Select names to be added in Available address list, and click the **Add>>** button to add them to the Selected address list.

Step 4. **Remove members:** Select names to be removed in the Selected Address list, and click the **<<Remove** button to remove these members from Selected Address list.

Step 5. Click **OK** to add the new group or click Cancel to discard changes.



Add New Address Group

Name:

< --- Available address --->
sebastien

< --- Selected address --->

Modifying a LAN Group

Step 1. In the LAN **Group** window, locate the network group desired to be modified and click its corresponding **Modify** option in the **Configure** field.

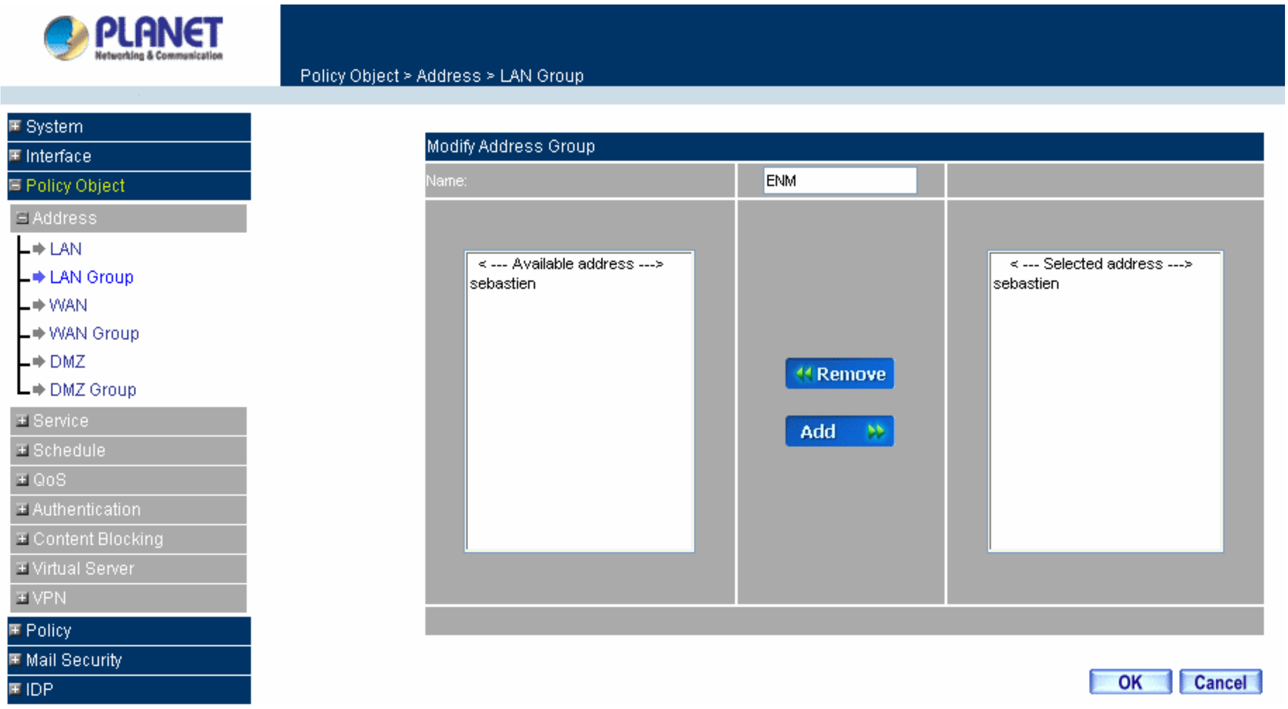
Step 2. A window displaying the information of the selected group appears:

- **Available address:** list names of all members of the LAN network.
- **Selected address:** list names of members which have been assigned to this group.

Step 3. **Add members:** Select names in **Available address** list, and click the **Add>>** button to add them to the **Selected address** list.

Step 4. **Remove members:** Select names in the **Selected address** list, and click the **<<Remove** button to remove these members from the **Selected address** list.

Click **OK** to save changes or click **Cancel** to discard changes.



Modify Address Group

Name: ENM

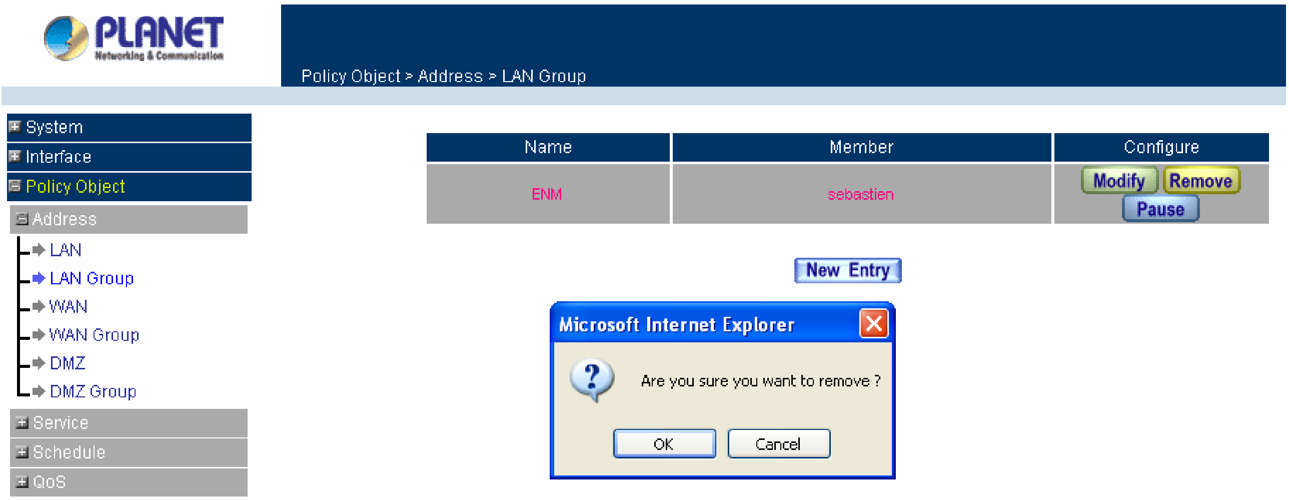
< --- Available address --->
sebastien

< --- Selected address --->
sebastien

Removing a LAN Group

Step 1. In the LAN **Group** window, locate the group to be removed and click its corresponding **Remove** option in the **Configure** field.

Step 2. In the **Remove** confirmation pop-up box, click **OK** to remove the group or click **Cancel** to discard changes.



Policy Object > Address > LAN Group

Name	Member	Configure
ENM	sebastien	Modify Remove Pause

New Entry

Microsoft Internet Explorer

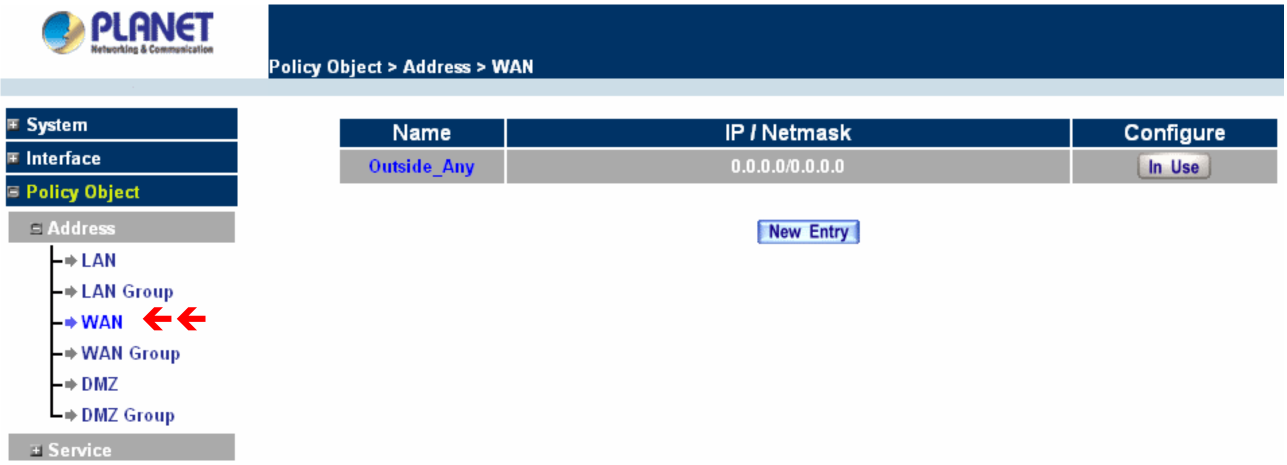
Are you sure you want to remove ?

OK Cancel

4.3.1.3 WAN

Entering the WAN window

Step 1. Click **WAN** under the **Address** menu to enter the WAN window. The current setting information, such as the name of the WAN network, IP and Netmask addresses will show on the screen.



Policy Object > Address > WAN

Name	IP / Netmask	Configure
Outside_Any	0.0.0.0/0.0.0.0	In Use

New Entry

Definitions

Name: Name of WAN network address.

IP/Netmask: IP address/Netmask of WAN network.

Configure: Configure the settings of WAN network. Click **Modify** to change the settings of WAN network. Click **Remove** to delete the setting of WAN network.

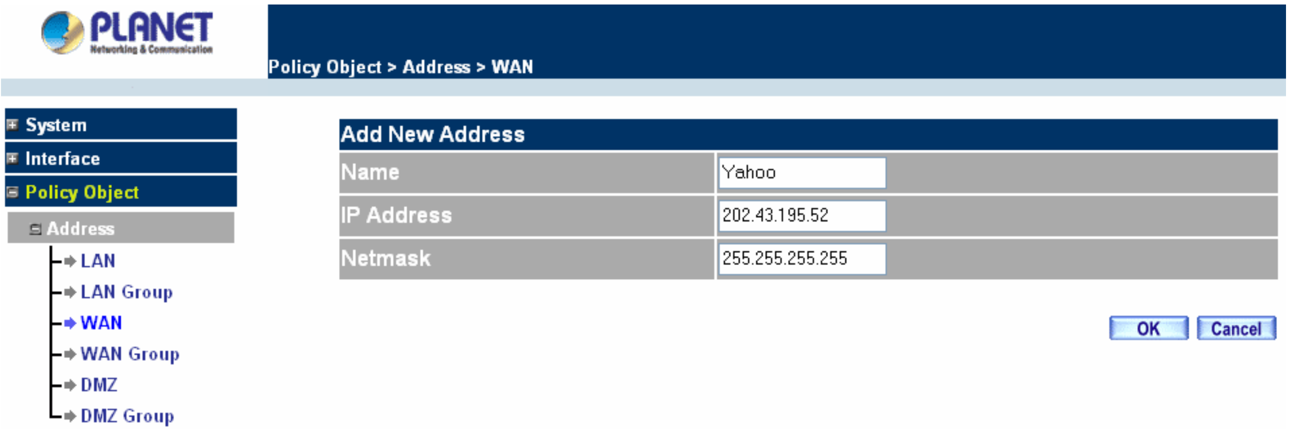
NOTE: In the WAN Network window, if one of the members has been added to **Policy** or **LAN Group**, the **Configure** column will show the message – **In Use**. In this case you are not allowed to modify or remove the settings.

Adding a new WAN Address

Step 1. In the WAN window, click the **New Entry** button.

Step 2. In the **Add New Address** window, enter the settings for a new WAN network address.

Step 3. Click **OK** to add the specified WAN network or click **Cancel** to discard changes.



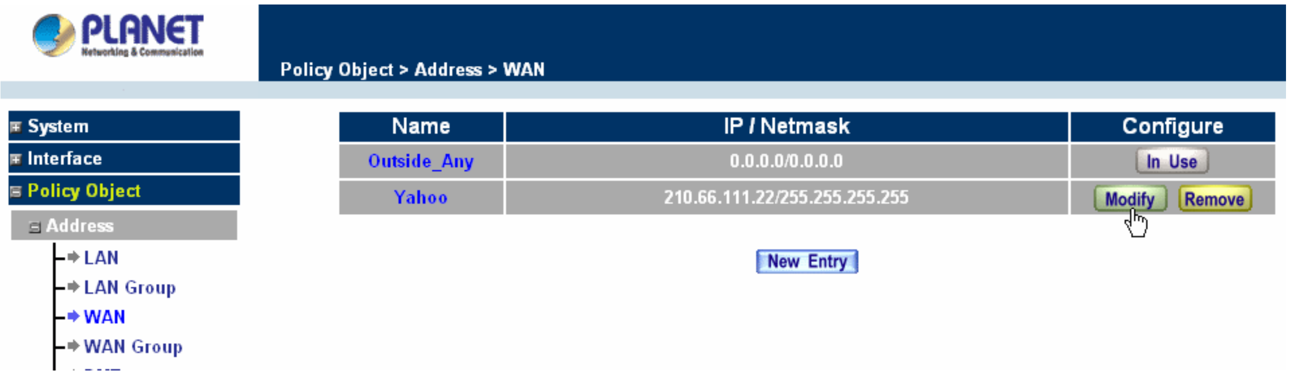
Add New Address	
Name	Yahoo
IP Address	202.43.195.52
Netmask	255.255.255.255

Modifying an WAN Address

Step 1. In the WAN table, locate the name of the network to be modified and click the **Modify** option in its corresponding **Configure** field.

Step 2. The **Modify Address** window will appear on the screen immediately. In the **Modify Address** window, fill in new addresses.

Step 3. Click **OK** to save changes or click **Cancel** to discard changes.

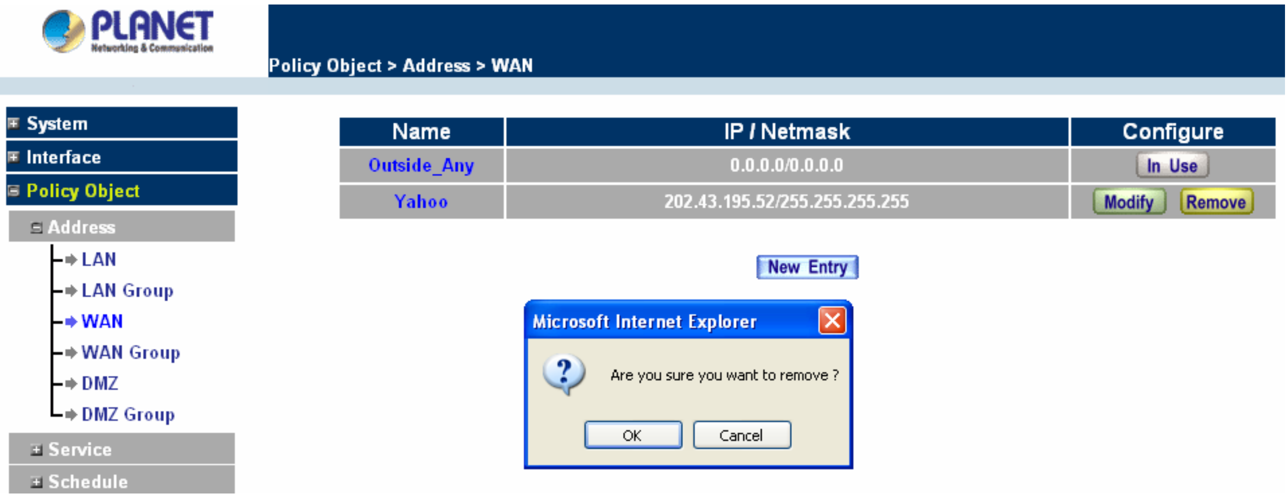


Name	IP / Netmask	Configure
Outside_Any	0.0.0.0/0.0.0.0	In Use
Yahoo	210.66.111.22/255.255.255.255	Modify Remove

Removing an WAN Address

Step 1. In the WAN table, locate the name of the network to be removed and click the **Remove** option in its corresponding Configure field.

Step 2. In the Remove confirmation pop-up box, click **OK** to remove the address or click **Cancel** to discard changes.



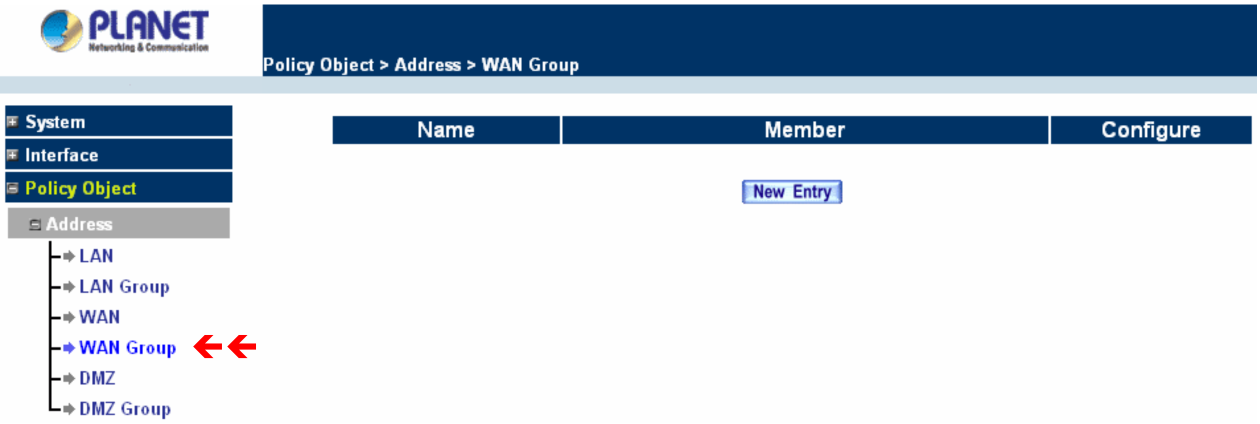
Name	IP / Netmask	Configure
Outside_Any	0.0.0.0/0.0.0.0	In Use
Yahoo	202.43.195.52/255.255.255.255	Modify Remove

Are you sure you want to remove ?

4.3.1.4 WAN Group

Entering the WAN Group window

Step 1. Click the **WAN Group** under the **Address** menu bar to enter the WAN window. The current settings for the WAN network group(s) will appear on the screen.



Name	Member	Configure

Definitions:

Name: Name of the WAN group.

Member: Members of the group.

Configure: Configure the settings of WAN group. Click **Modify** to change the parameters of WAN group Click Remove to delete the selected group.

NOTE: In the **WAN Group** window, if one of the members has been added to the **Policy**, “**In Use**” message will appear in the **Configure** column. You are not allowed to modify or remove the settings. Go to the **Policy** window to remove the setting, and then you can configure.

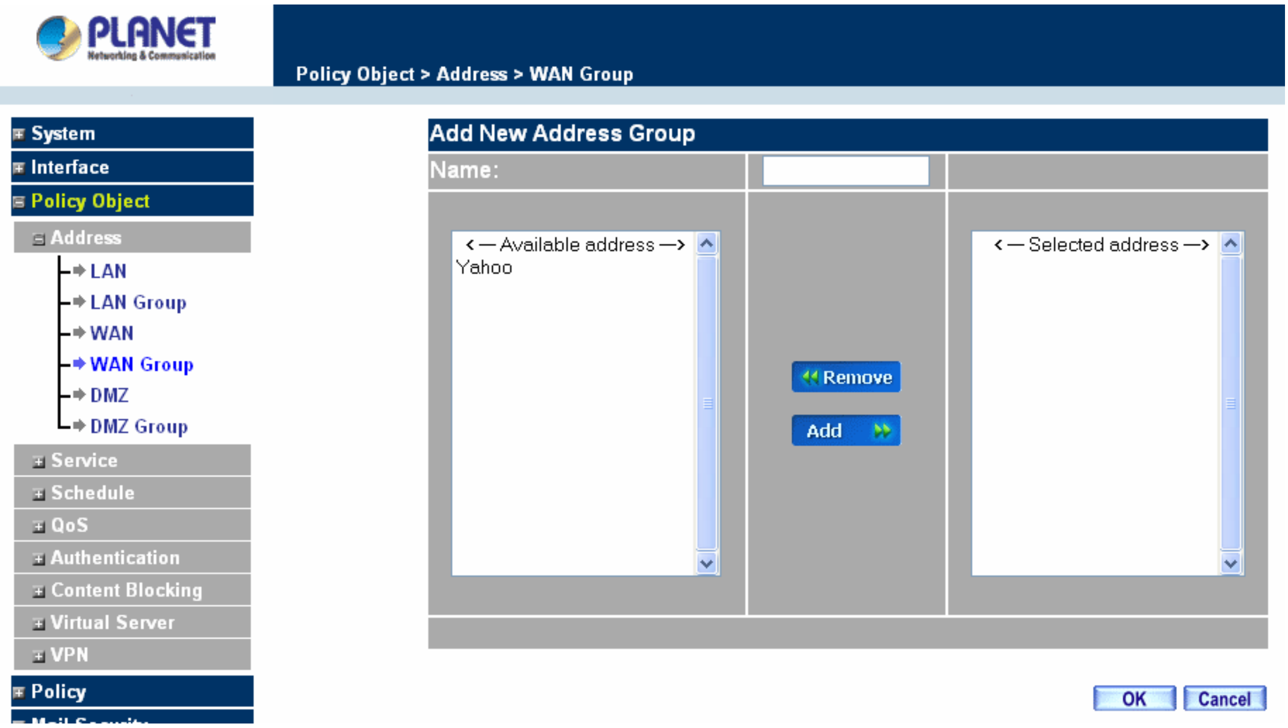
Adding an WAN Group

Step 1. In the **WAN Group** window, click the **New Entry** button and the **Add New Address Group** window will appear.

Step 2. In the **Add New Address Group** window the following fields will appear:

- **Name:** enter the name of the new group.
- **Available address:** List the names of all the members of the WAN network.
- **Selected address:** List the names to assign to the new group.
- **Add members:** Select the names to be added in the **Available address** list, and click the **Add>>** button to add them to the **Selected address** list.
- **Remove members:** Select the names to be removed in the **Selected address** list, and click the **<<Remove** button to remove them from the **Selected address** list.

Step 3. Click **OK** to add the new group or click **Cancel** to discard changes.



Modifying a WAN Group

Step 1. In the **WAN Group** window, locate the network group to be modified and click its corresponding **Modify** button in the **Configure** field.

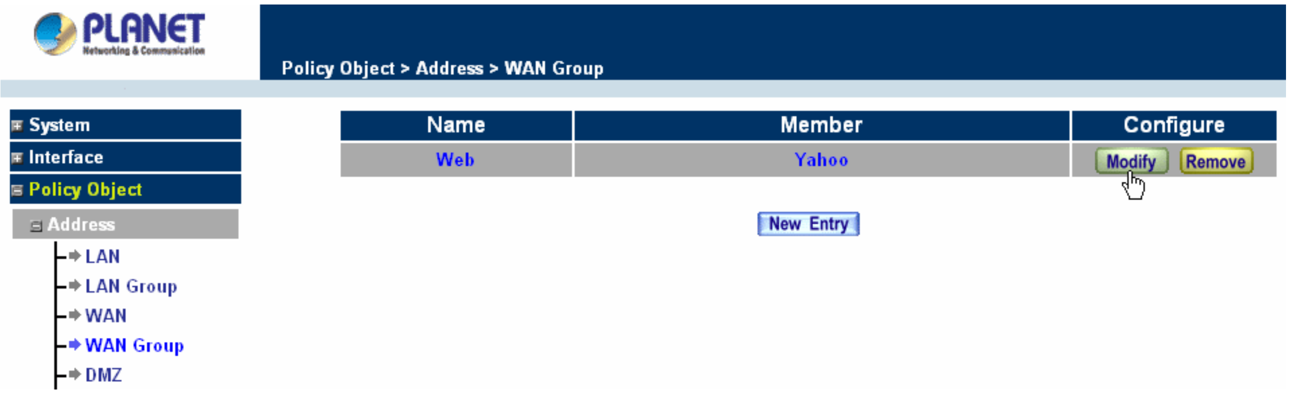
Step 2. A window displaying the information of the selected group appears:

- **Available address:** list the names of all the members of the WAN network.
- **Selected address:** list the names of the members that have been assigned to this group.

Step 3. **Add members:** Select the names to be added in the **Available address** list, and click the **Add>>** button to add them to the **Selected address** list.

Step 4. **Remove members:** Select the names to be removed in the **Selected address** list, and click the **<<Remove** button to remove them from the **Selected address** list.

Step 5. Click **OK** to save changes or click **Cancel** to discard changes.

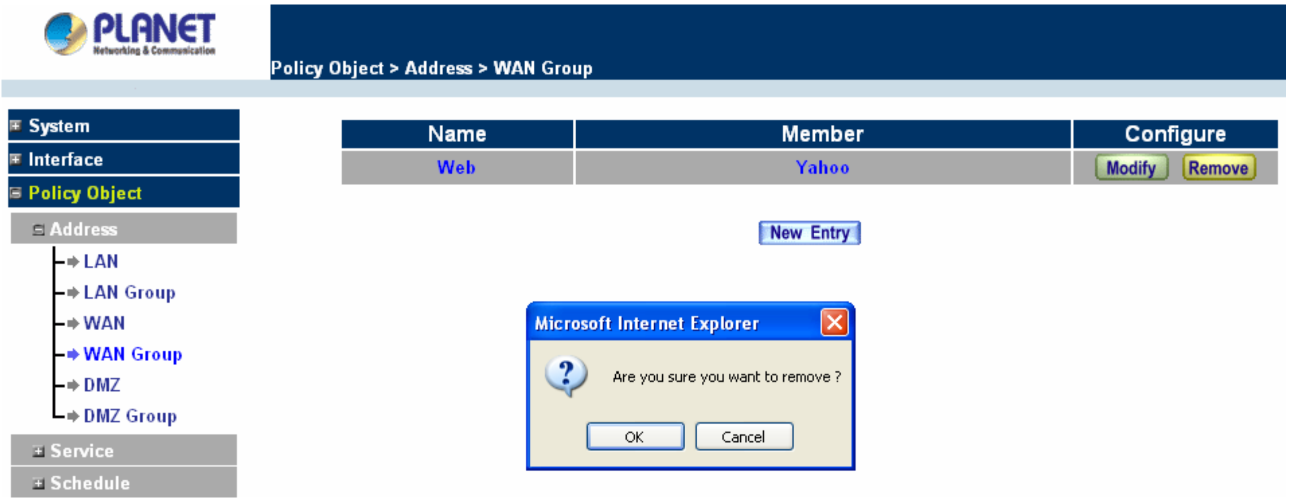


Name	Member	Configure
Web	Yahoo	Modify Remove

Removing a WAN Group

Step 1. In the **WAN Group** window, locate the group to be removed and click its corresponding **Modify** option in the **Configure** field.

Step 2. In the **Remove confirmation** pop-up box, click **OK** to remove the group or click **Cancel** to discard changes.



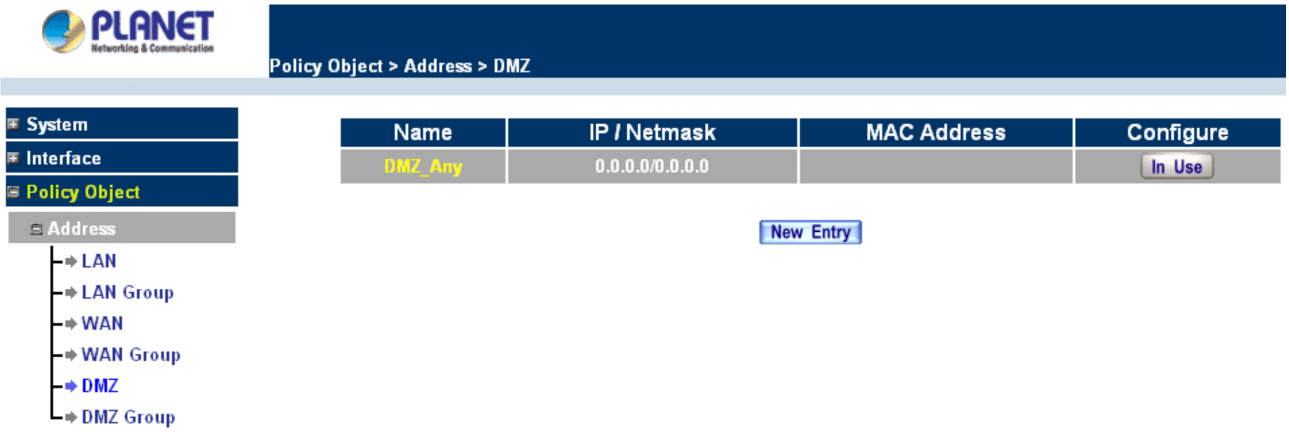
Name	Member	Configure
Web	Yahoo	Modify Remove

Are you sure you want to remove ?

4.3.1.5 DMZ

Entering the DMZ window:

Click **DMZ** under the **Address** menu to enter the **DMZ** window. The current setting information such as the name of the LAN network, IP, and Netmask addresses will show on the screen.



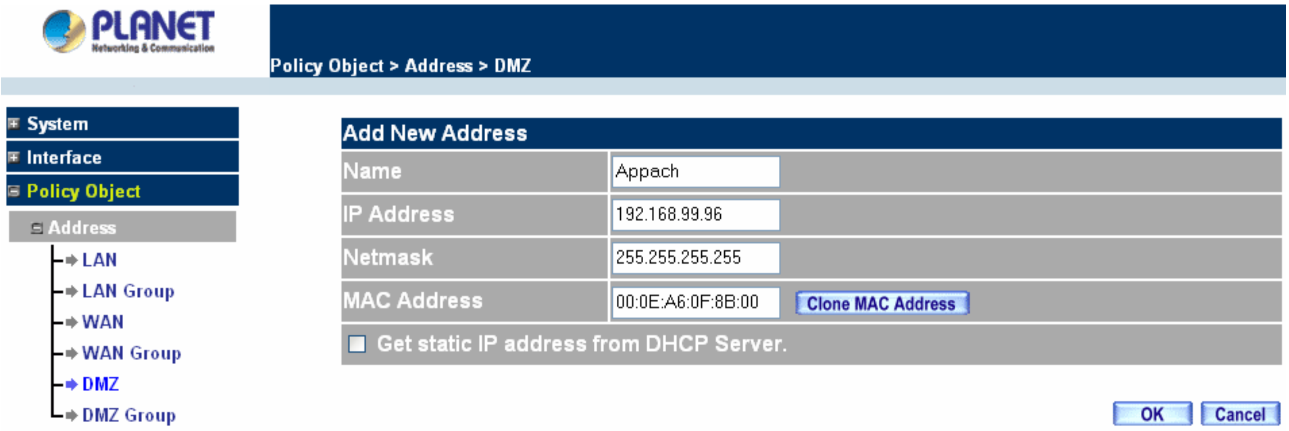
Name	IP / Netmask	MAC Address	Configure
DMZ_Any	0.0.0.0/0.0.0.0		In Use

Adding a new DMZ Address:

Step 1. In the DMZ window, click the **New Entry** button.

Step 2. In the **Add New Address** window, enter the settings for a new DMZ address.

Step 3. Click **OK** to add the specified DMZ or click **Cancel** to discard changes.



Add New Address	
Name	Appach
IP Address	192.168.99.96
Netmask	255.255.255.255
MAC Address	00:0E:A6:0F:8B:00

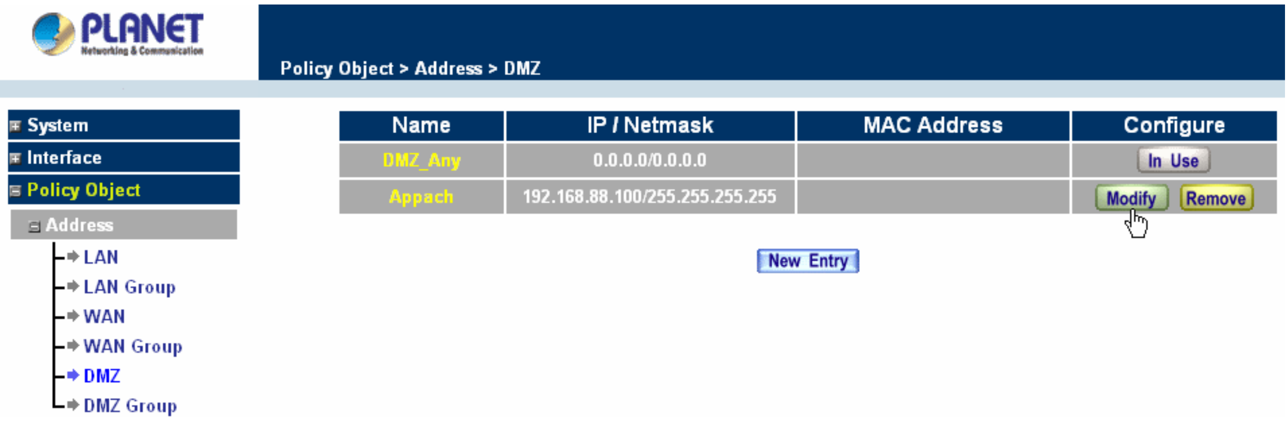
☐ Get static IP address from DHCP Server.

Modifying a DMZ Address:

Step 1. In the **DMZ** window, locate the name of the network to be modified and click the **Modify** option in its corresponding **Configure** field.

Step 2. In the **Modify Address** window, fill in new addresses.

Step 3. Click **OK** on save the changes or click **Cancel** to discard changes.

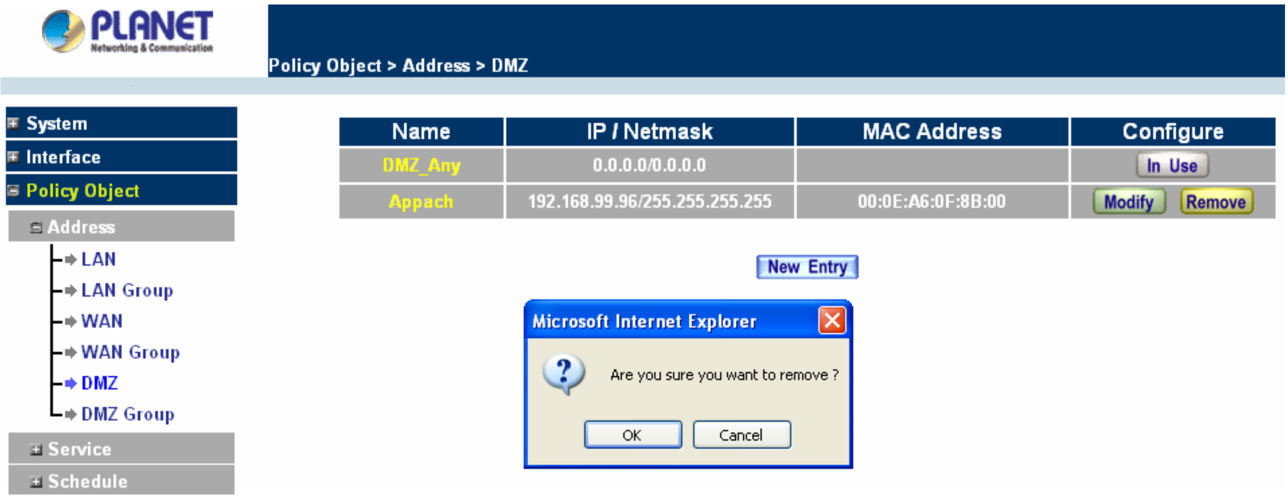


Name	IP / Netmask	MAC Address	Configure
DMZ_Any	0.0.0.0/0.0.0.0		In Use
Appach	192.168.88.100/255.255.255.255		Modify Remove

Removing a DMZ Address:

Step 1. In the **DMZ** window, locate the name of the network to be removed and click the **Remove** option in its corresponding **Configure** field.

Step 2. In the **Remove** confirmation pop-up box, click **OK** to remove the address or click **Cancel** to discard changes.



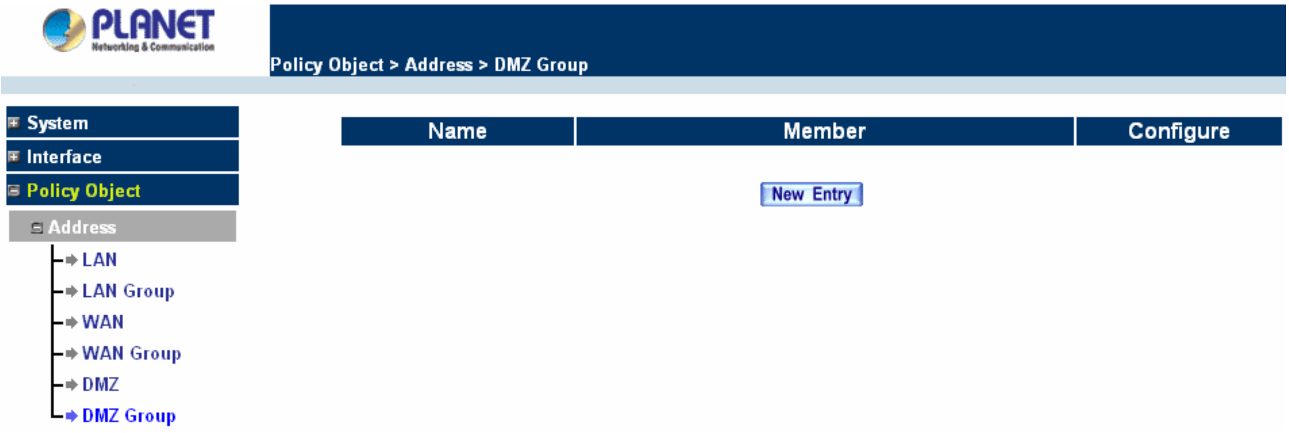
Name	IP / Netmask	MAC Address	Configure
DMZ_Any	0.0.0.0/0.0.0.0		In Use
Appach	192.168.99.96/255.255.255.255	00:0E:A6:0F:8B:00	Modify Remove

Are you sure you want to remove ?

4.3.1.6 DMZ Group

Entering the DMZ Group window

Click **DMZ Group** under the **Address** menu to enter the **DMZ** window. The current settings information for the DMZ group appears on the screen.



Adding a DMZ Group:

Step 1. In the DMZ Group window, click the **New Entry** button.

Step 2. In the **Add New Address** Group window:

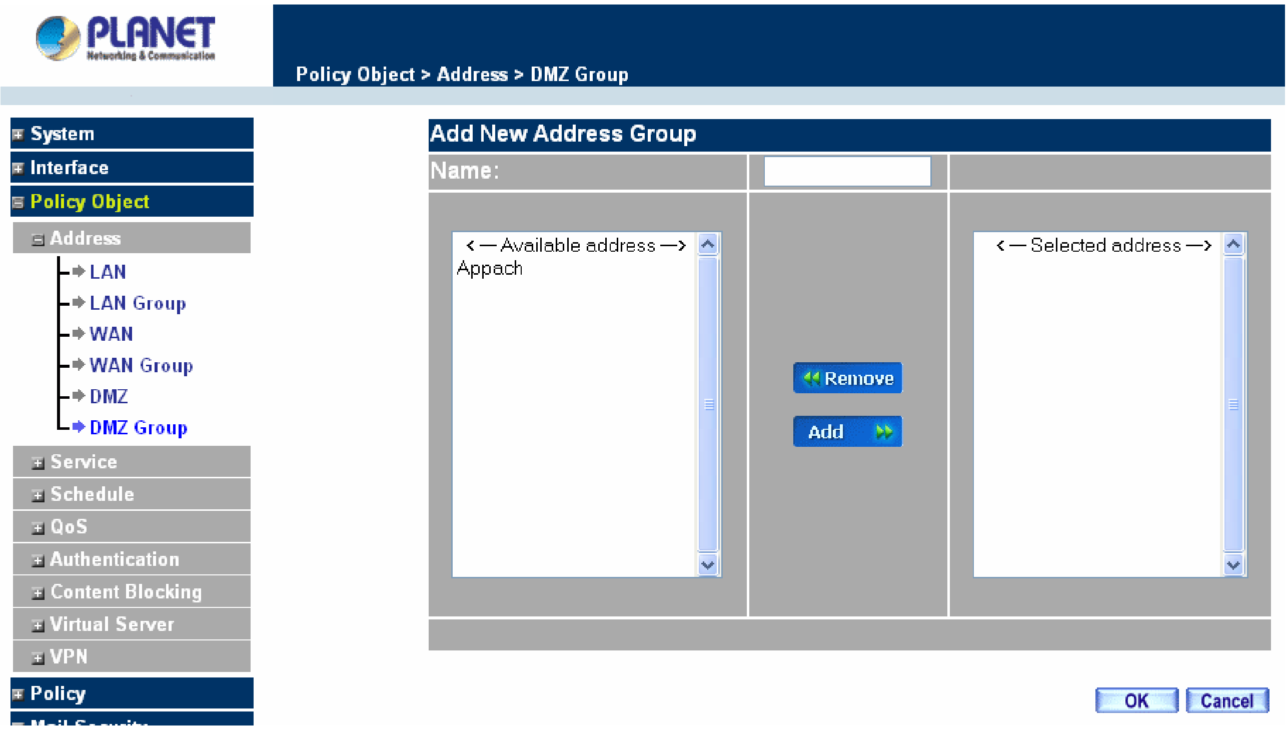
- **Available address:** list names of all members of the DMZ.
- **Selected address:** list names to assign to a new group.

Step 3. Name: enter a name for the new group.

Step 4. **Add members:** Select the names to be added from the **Available address** list, and click the **Add>>** button to add them to the **Selected address** list.

Step 5. **Remove members:** Select names to be removed from the **Selected address** list, and click the **<<Remove** button to remove them from the **Selected address** list.

Step 6. Click **OK** to add the new group or click **Cancel** to discard changes.



Modifying a DMZ Group:

Step 1. In the **DMZ** Group window, locate the **DMZ** group to be modified and click its corresponding **Modify** button in the **Configure** field.

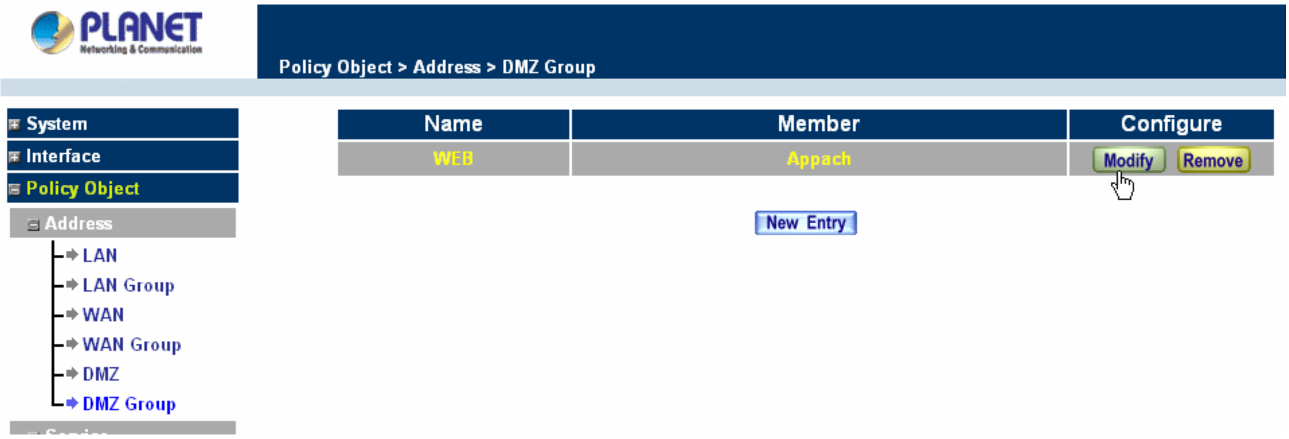
Step 2. A window displaying information about the selected group appears:

- **Available address:** list the names of all the members of the DMZ.
- **Selected address:** list the names of the members that have been assigned to this group.

Step 3. **Add members:** Select names to be added from the a**vailable Address** list, and click the **Add>>** button to add them to the **Selected address** list.

Step 4. **Remove members:** Select names to be removed from the **Selected address** list, and click the **<<Remove** button to remove them from **Selected address** list.

Step 5. Click **OK** to save changes or click Cancel to cancel editing.



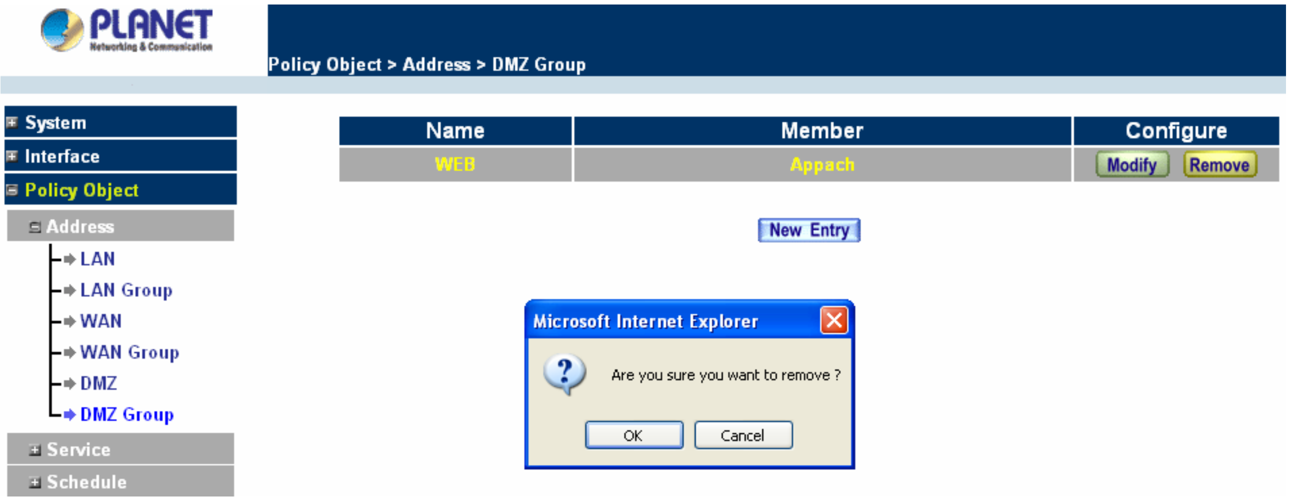
Policy Object > Address > DMZ Group

Name	Member	Configure
WEB	Appach	Modify Remove

Removing a DMZ Group:

Step 1. In the **DMZ Group** window, locate the group to be removed and click its corresponding **Remove** option in the **Configure** field.

Step 2. In the **Remove confirmation** pop-up box, click **OK** to remove the group.



Policy Object > Address > DMZ Group

Name	Member	Configure
WEB	Appach	Modify Remove

Microsoft Internet Explorer

Are you sure you want to remove ?

4.3.2 Service

In this section, network services are defined and new network services can be added. There are three sub menus under Service which are: **Pre-defined**, **Custom**, and **Group**. The Administrator can simply follow the instructions below to define the protocols and port numbers for network communication applications. Users then can connect to servers and other computers through these available network services.

What is Service?

TCP and UDP protocols support varieties of services, and each service consists of a TCP Port or UDP port number, such as TELNET(23), SMTP(21), POP3(110),etc. The Content Security Gateway defines two services: pre-defined service and custom service. The common-use services like TCP and UDP are defined in the pre-defined service and cannot be modified or removed. In the custom menu, users can define other TCP port and UDP port numbers that are not in the pre-defined menu according to their needs. When defining custom services, the client port ranges from 1024 to 65535 and the server port ranges from 0 to 1023.

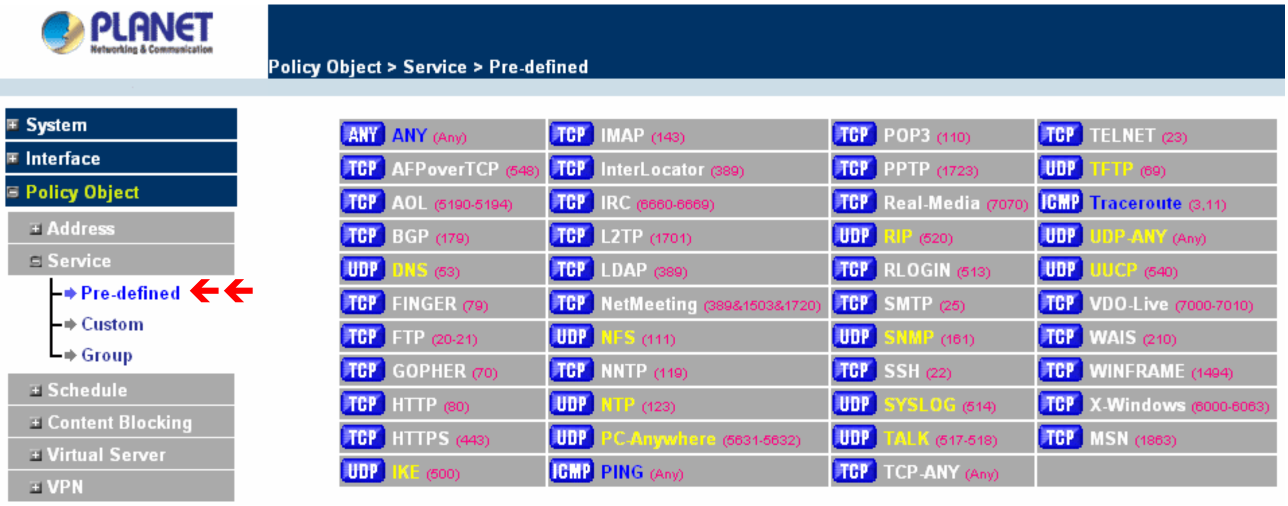
How do I use Service?

The Administrator can add new service group names in the **Group** option under **Service** menu, and assign desired services into that new group. Using service group the Administrator can simplify the processes of setting up control policies. For example, there are 10 different computers that want to access 5 different services on a server, such as HTTP, FTP, SMTP, POP3, and TELNET. Without the help of service groups, the Administrator needs to set up 50 (10x5) control policies, but by applying all 5 services to a single group name in the **service** field, it takes only one control policy to achieve the same effect as the 50 control policies.

4.3.2.1 Pre-defined

Entering a Pre-defined window

Step 1. Click **Pre-defined** under it. A window will appear with a list of services and their associated IP addresses. This list cannot be modified.



ANY ANY (Any)	TCP IMAP (143)	TCP POP3 (110)	TCP TELNET (23)
TCP AFPoverTCP (548)	TCP InterLocator (389)	TCP PPTP (1723)	UDP TFTP (69)
TCP AOL (5190-5194)	TCP IRC (6660-6669)	TCP Real-Media (7070)	ICMP Traceroute (3,11)
TCP BGP (179)	TCP L2TP (1701)	UDP RIP (520)	UDP UDP-ANY (Any)
UDP DNS (53)	TCP LDAP (389)	TCP RLOGIN (513)	UDP UUCP (540)
TCP FINGER (79)	TCP NetMeeting (389&1503&1720)	TCP SMTP (25)	TCP VDO-Live (7000-7010)
TCP FTP (20-21)	UDP NFS (111)	UDP SNMP (161)	TCP WAIS (210)
TCP GOPHER (70)	TCP NNTP (119)	TCP SSH (22)	TCP WINFRAME (1494)
TCP HTTP (80)	UDP NTP (123)	UDP SYSLOG (514)	TCP X-Windows (6000-6063)
TCP HTTPS (443)	UDP PC-Anywhere (5631-5632)	UDP TALK (517-518)	TCP MSN (1863)
UDP IKE (500)	ICMP PING (Any)	TCP TCP-ANY (Any)	

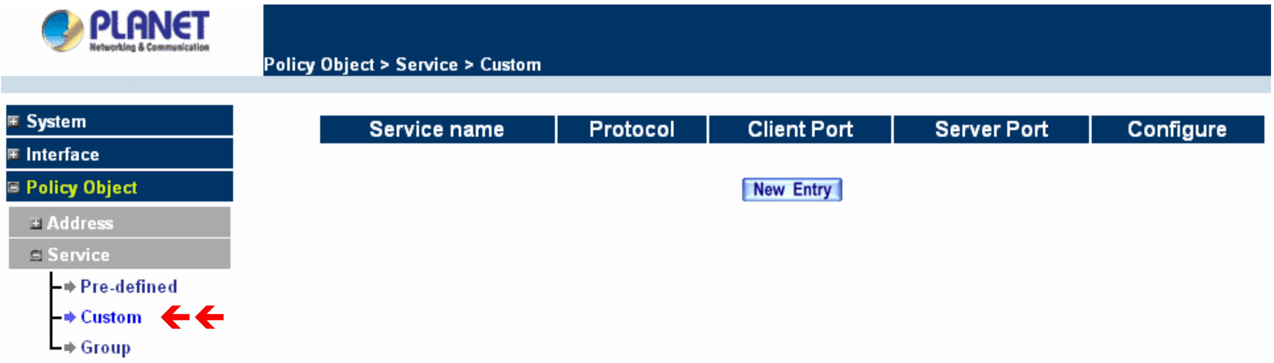
Icons and Descriptions

Figur	Description
TCP	TCP services, e.g. AFPoverTCP, AOL, BGP, FINGER, FTP, GOPHER, HTTP, HTTPS, IMAP, InterLocator, IRC, L2TP, LDAP, NetMeeting, NNTP, POP3, PPTP, Real-Media, RLOGIN, SMTP, SSH, TCP ANY, TELNET, VDO Live, WAIS, WINFRAME, X-WINDOWS, MSN, etc.
UDP	UDP services, e.g. DNS, IKE, NFS, NTP, PC-Anywhere, RIP, SNMP, SYSLOG, TALK, TFTP, UDP-ANY, UUCP, etc.
ICMP	ICMP services, i.g. PING, TRACEROUTE, etc.

4.3.2.2 Custom

Entering the Custom window

Step 1. Click **Custom** under it. A window will appear with a table showing all services currently defined by the Administrator.



Service name	Protocol	Client Port	Server Port	Configure

Definitions:

Service name: The defined service name.

Protocol: Network protocol used in the basic setting. Such as TCP、UDP or others.

Client port: The range of Client port in defined service. If the number of ports entered in the two fields of Client port is different, it means that the port numbers between these two numbers are opened. If the number of ports entered in the two fields of Client port is identical, it means that the entered port number is opened.

Service port: The range of Service port in defined service.

If the number of ports entered in the two fields of Service port is different, it means that the port numbers between these two numbers are opened. If the number of ports entered in the two fields of Service port is identical, it means that the entered port number is opened.

Configure: Configure the settings in Service table. Click **Modify** to change the parameters in Service table. Click **Remove** to delete the selected setting.

NOTE: In the **Custom** window, if one of the services has been added to **Policy** or **Group**, "**In Use**" message will appear in the **Configure** column. In this case you are not allowed to modify or remove the settings. Go to the **Policy** or **Group** window to delete the setting, and then you can configure the settings.

Adding a new Service

In the **Custom** window, click the **New Entry** button and a new service table appears.

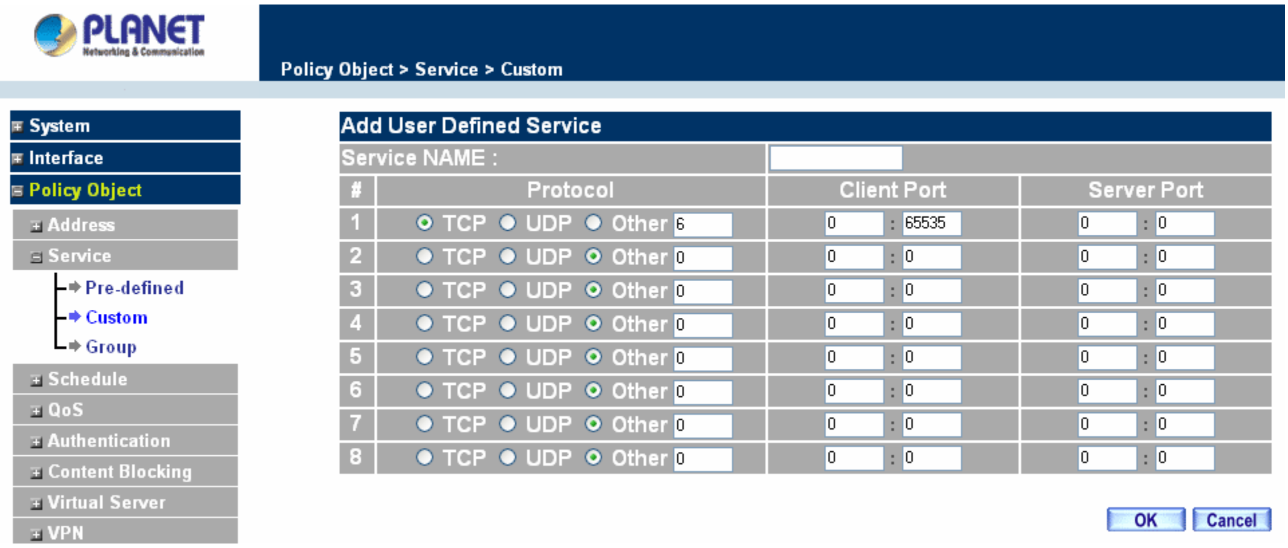
In the new service table:

- New Service Name: This will be the name referencing the new service.
- Protocol: Enter the network protocol type to be used, such as TCP, UDP, or Other (please enter the number for the protocol type).
- Client Port: enter the range of port number of new clients.
- Server Port: enter the range of port number of new servers.

The client port ranges from 1024 to 65535 and the server port ranges from 0 to 1023.

Step 1. Click **New Entry** to add new services.

Step 2. Click **OK** to accept editing; or click **Cancel**.



Add User Defined Service

Service NAME :

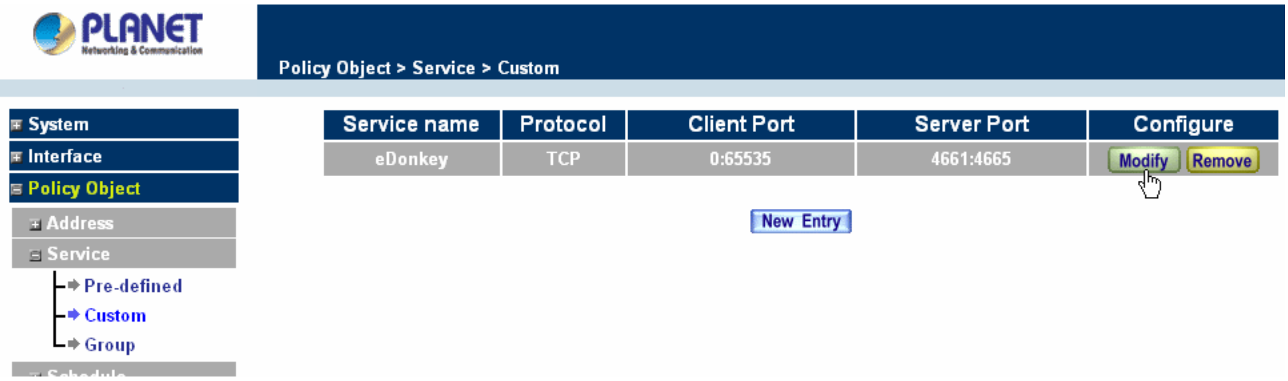
#	Protocol	Client Port	Server Port
1	● TCP ○ UDP ○ Other 6	0 : 65535	0 : 0
2	○ TCP ○ UDP ● Other 0	0 : 0	0 : 0
3	○ TCP ○ UDP ● Other 0	0 : 0	0 : 0
4	○ TCP ○ UDP ● Other 0	0 : 0	0 : 0
5	○ TCP ○ UDP ● Other 0	0 : 0	0 : 0
6	○ TCP ○ UDP ● Other 0	0 : 0	0 : 0
7	○ TCP ○ UDP ● Other 0	0 : 0	0 : 0
8	○ TCP ○ UDP ● Other 0	0 : 0	0 : 0

Modifying Custom Services

Step 1. A table showing the current settings of the selected service appears on the screen

Step 2. Enter the new values.

Step 3. Click **OK** to accept editing; or click **Cancel**.

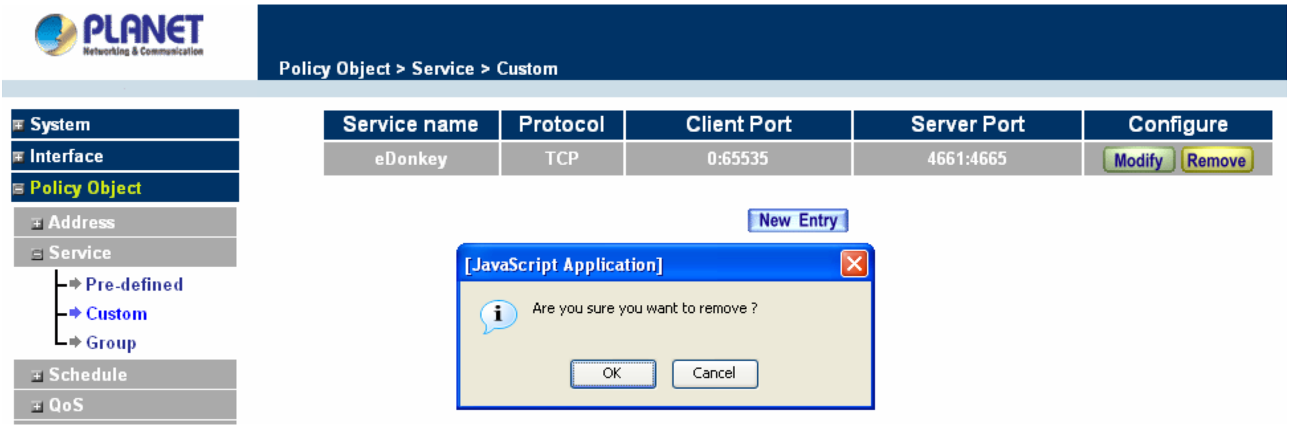


Service name	Protocol	Client Port	Server Port	Configure
eDonkey	TCP	0:65535	4661:4665	Modify Remove

Removing Custom Services

Step 1. Click its corresponding **Remove** option in the **Configure** field.

Step 2. In the **Remove** confirmation pop-up box, click **OK** to remove the selected service or click **Cancel** to cancel action.



Service name	Protocol	Client Port	Server Port	Configure
eDonkey	TCP	0:65535	4661:4665	Modify Remove

[JavaScript Application]

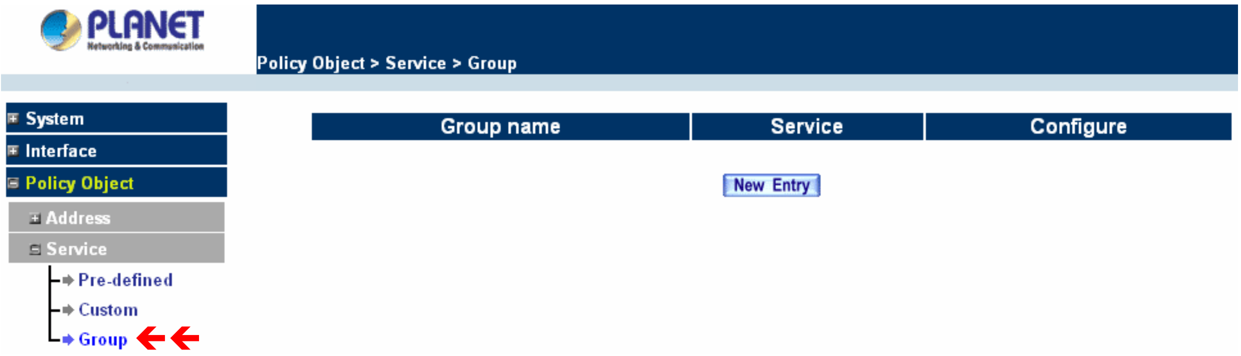
Are you sure you want to remove ?

OK Cancel

4.3.2.3 Group

Accessing the Group window

Step 1. Click **Group** under it. A window will appear with a table displaying current service group settings set by the Administrator.



Group name	Service	Configure

Definitions:

Group name: The Group name of the defined Service.

Service: The Service item of the Group.

Configure: Configure the settings of Group. Click **Modify** to change the parameters of the Group. Click Remove to delete the Group.

NOTE: In the **Group** window, if one of the Service Groups has been added to **Policy**. "**In Use**" message will appear in the **Configure** column. You are not allowed to modify or remove the settings. Go to the Policy window, remove the Service group first, and then you are allowed to configure the setting.

Adding Service Groups

Step 1. In the **Group** window, click the **New Entry** button.

Step 2. In the **Add Service Group** window, the following fields will appear:

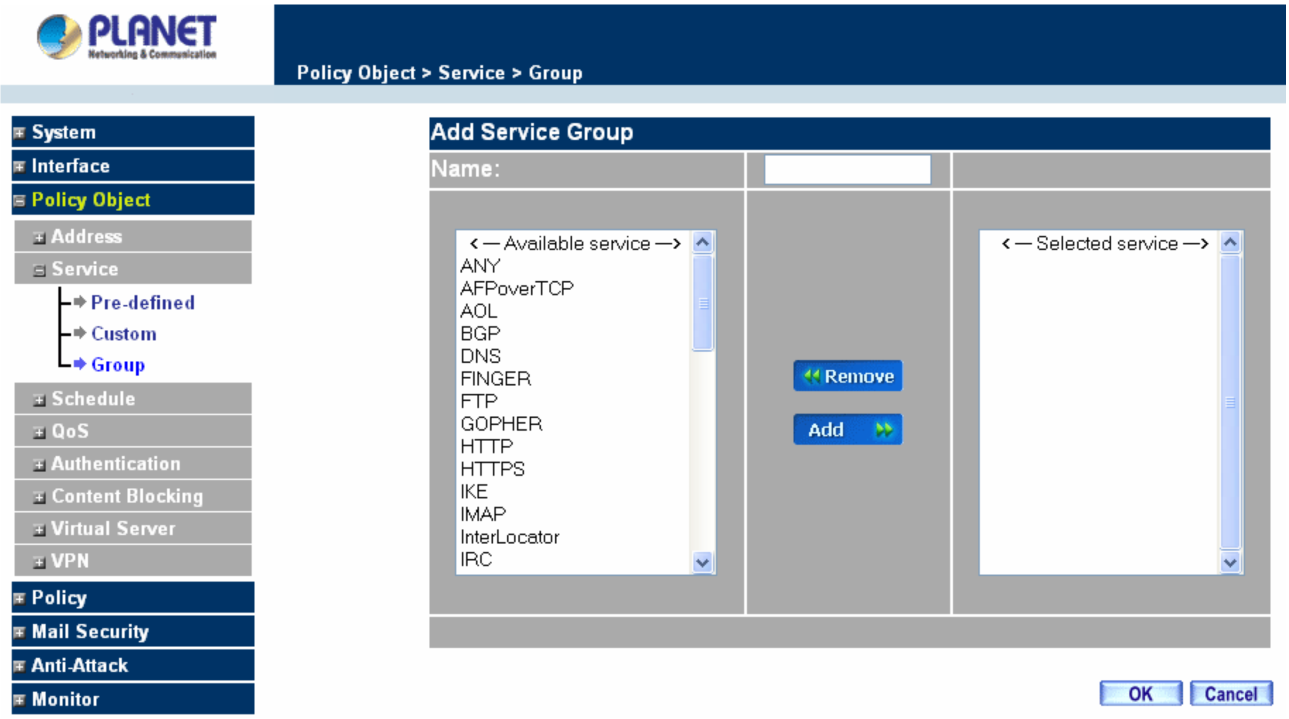
- **Available service:** list all the available services.
- **Selected service:** list services to be assigned to the new group.

Step 3. Enter the new group name in the group **Name** field. This will be the name referencing the created group.

Step 4. **To add new services:** Select the services desired to be added in the **Available service** list and then click the **Add>>** button to add them to the group.

Step 5. **To remove services:** Select services desired to be removed in the **Available service**, and then click the **<<Remove** button to remove them from the group.

Step 6. Click **OK** to add the new group.



Modifying Service Groups

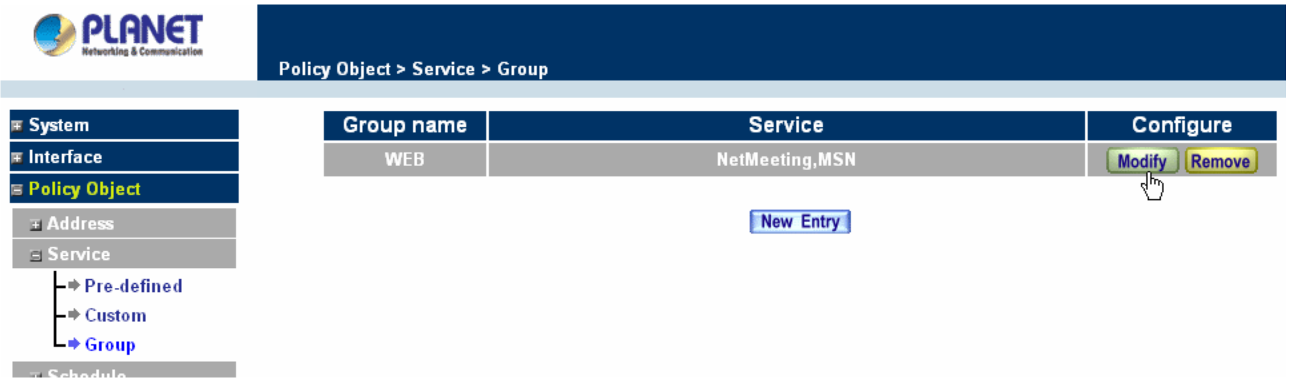
Step 1. In the Mod (modify) group window the following fields are displayed:

- **Available service:** lists all the available services.
- **Selected service:** list services that have been assigned to the selected group.

Step 2. **Add new services:** Select services in the **Available service** list, and then click the **Add>>** button to add them to the group.

Step 3. **Remove services:** Select services to be removed in the **Selected service** list, and then click the **<<Remove** button to remove theses services from the group.

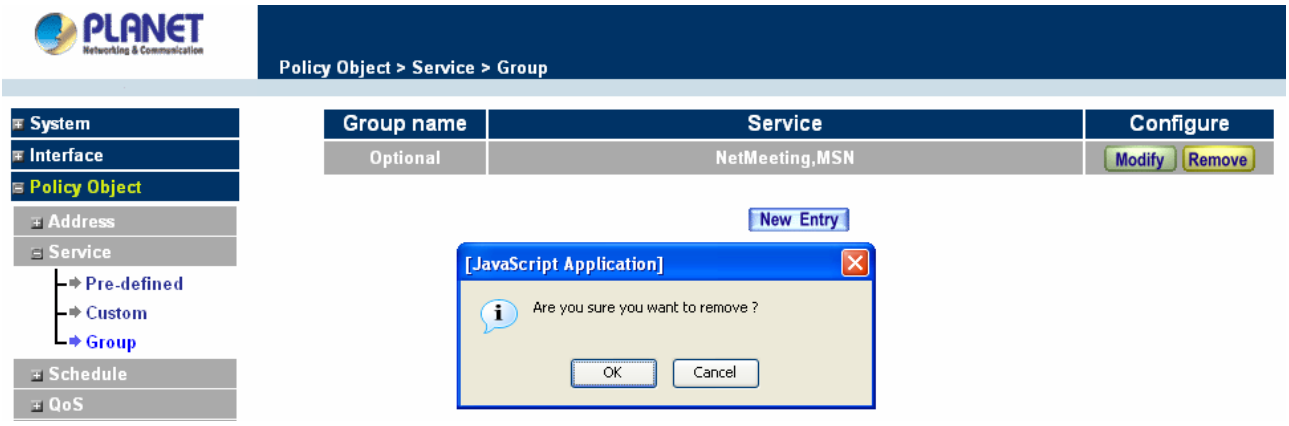
Step 4. Click **OK** to save editing changes.



Group name	Service	Configure
WEB	NetMeeting,MSN	Modify Remove

Removing Service Groups

In the **Remove** confirmation pop-up box, click **OK** to remove the selected service group or click **Cancel** to cancel removing.



Group name	Service	Configure
Optional	NetMeeting,MSN	Modify Remove

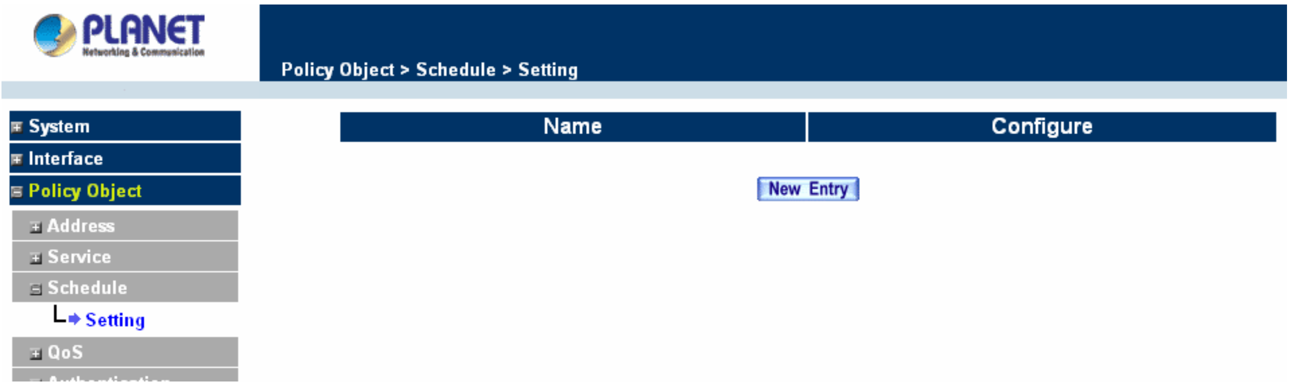
Are you sure you want to remove ?

4.3.3 Schedule

The Content Security Gateway allows the Administrator to configure a schedule for policies to take affect. By creating a schedule, the Administrator is allowing the Content Security Gateway policies to be used at those designated times only. Any activities outside of the scheduled time slot will not follow the Content Security Gateway policies therefore will likely not be permitted to pass through the Content Security Gateway. The Administrator can configure the start time and stop time, as well as creating 2 different time periods in a day. For example, an organization may only want the Content Security Gateway to allow the LAN network users to access the Internet during work hours. Therefore, the Administrator may create a schedule to allow the Content Security Gateway to work Monday-Friday, 8AM - 5PM only. During the non-work hours, the Content Security Gateway will not allow Internet access.

Accessing the Schedule window

Step 1. Click on **Setting** on the **Schedule** menu bar and the schedule window will appear displaying the active schedules.



Name	Configure

New Entry

The following items are displayed in this window:

Name: the name assigned to the schedule

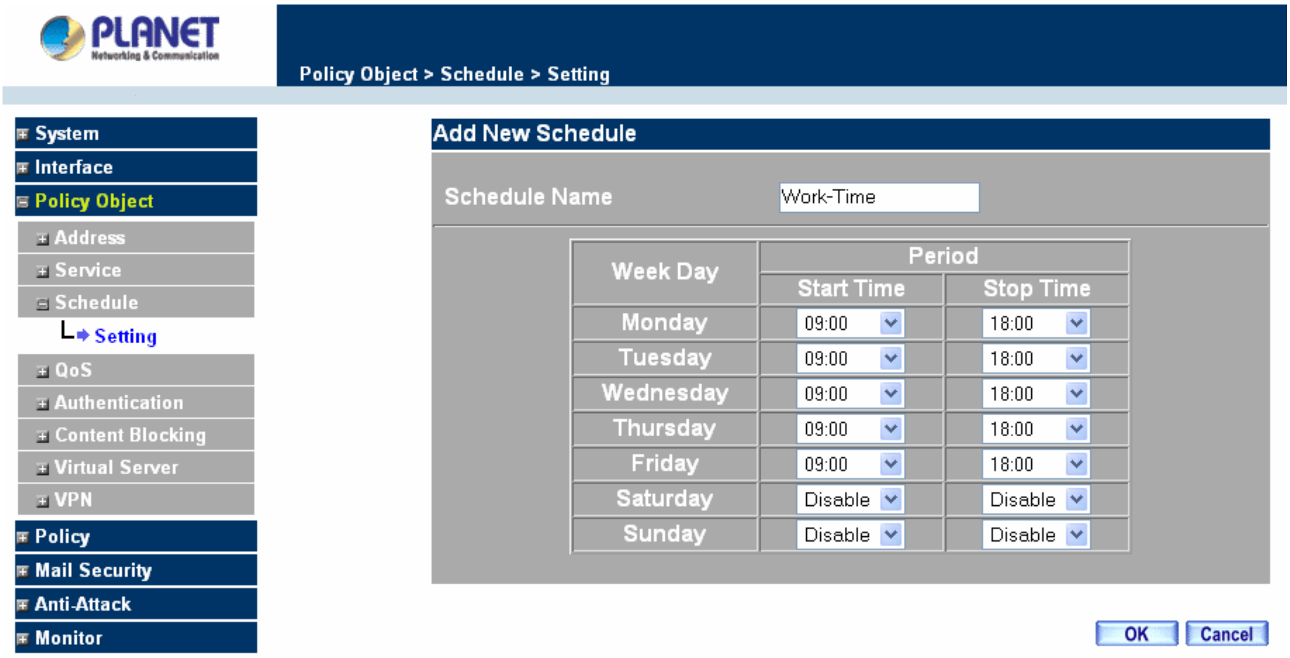
Configure: modify or remove

Adding a new Schedule

Step 1. Click on the **New Entry** button and the **Add New Schedule** window will appear.

- **Schedule Name:** Fill in a name for the new schedule.
- **Period:** Configure the start and stop time for the days of the week that the schedule will be active.

Step 2. Click **OK** to save the new schedule or click Cancel to cancel adding the new schedule.



Add New Schedule

Schedule Name: Work-Time

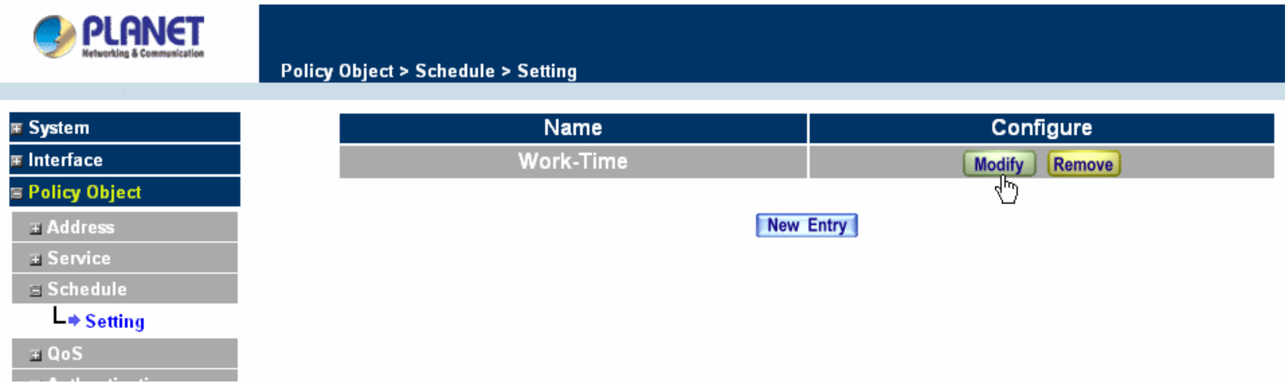
Week Day	Period	
	Start Time	Stop Time
Monday	09:00	18:00
Tuesday	09:00	18:00
Wednesday	09:00	18:00
Thursday	09:00	18:00
Friday	09:00	18:00
Saturday	Disable	Disable
Sunday	Disable	Disable

NOTE: In setting a Schedule, the value in **Start time** must be less than the value in **Stop Time**, or you cannot add or configure the setting.

Modifying a Schedule

Step 1. In the **Schedule** window, find the policy to be modified and click the corresponding **Modify** option in the **Configure** field. Make needed changes.

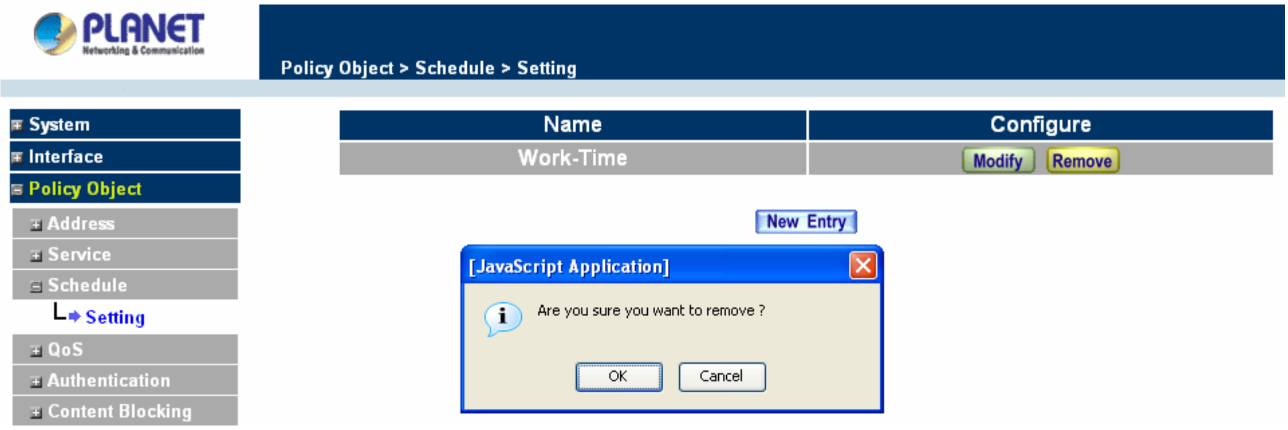
Step 2. Click **OK** to save changes.



Removing a Schedule

Step 1. In the **Schedule** window, find the policy to be removed and click the corresponding **Remove** option in the **Configure** field.

Step 2. A confirmation pop-up box will appear, click on **OK** to remove the schedule.



Are you sure you want to remove ?

4.3.4 QoS

By configuring the QoS, you can control the outbound Upstream/downstream Bandwidth.

The administrator can configure the bandwidth according to the WAN bandwidth.

Downstream Bandwidth: To configure the Guaranteed Bandwidth and Maximum Bandwidth.

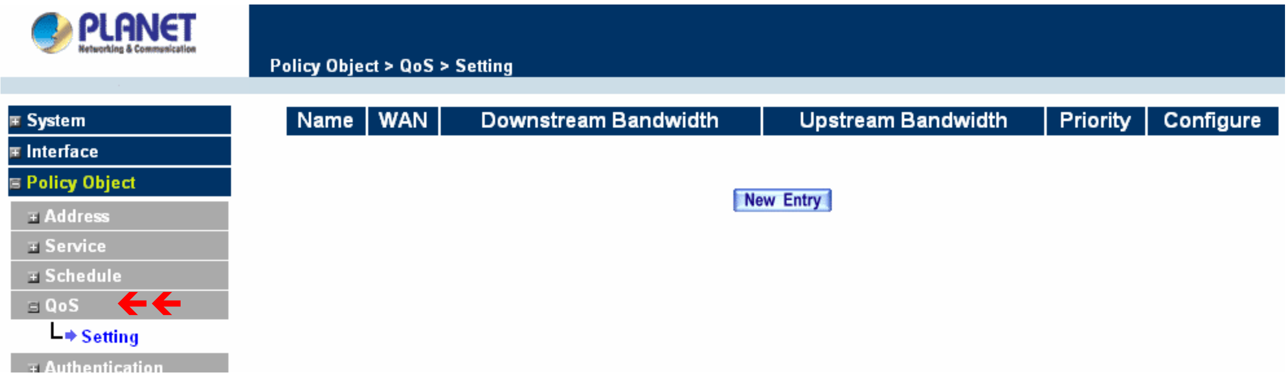
Upstream Bandwidth: To configure the Guaranteed Bandwidth and Maximum Bandwidth.

QoS Priority: To configure the priority of distributing Upstream/Downstream and unused bandwidth.

CS-500 configures the bandwidth by different QoS, and selects the suitable QoS through Policy to control and efficiently distribute bandwidth. CS-500 also makes it convenient for the administrator to use CS_500 with the best Utility.

Configuration of QoS

Click QoS in the menu bar on the left hand side.



Name	WAN	Downstream Bandwidth	Upstream Bandwidth	Priority	Configure

Definitions:

Name: The name of the QoS you want to configure.

WAN: Display WAN interface.

Downstream Bandwidth: To configure the Guaranteed Bandwidth and Maximum Bandwidth.

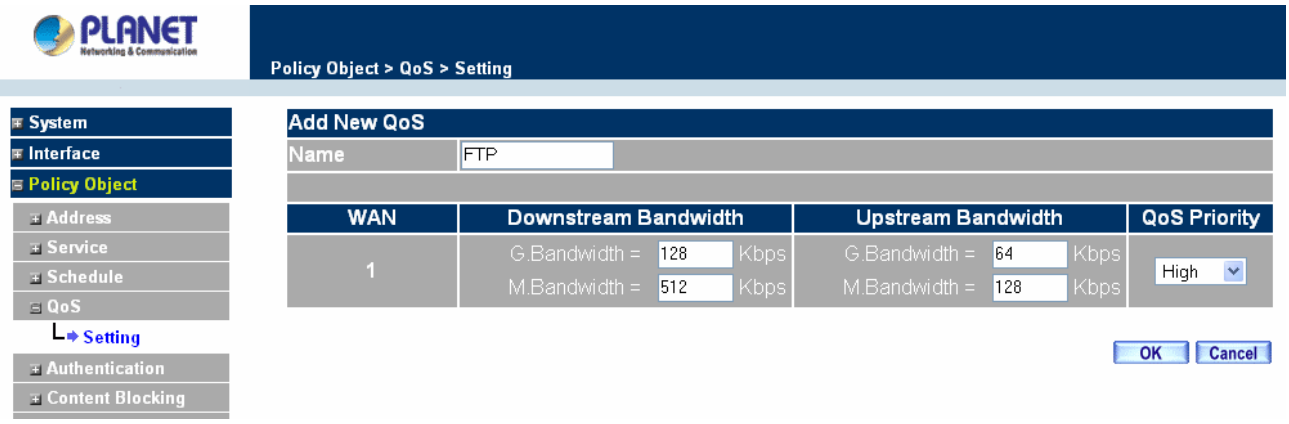
Upstream Bandwidth: To configure the Guaranteed Bandwidth and Maximum Bandwidth.

Priority: To configure the priority of distributing Upstream/Downstream and unused bandwidth.

Add New QoS

Step 1. Click QoS in the menu bar on the left hand side.

Step 2. Click the **New Entry** button to add new QoS.



Add New QoS

Name: FTP

WAN	Downstream Bandwidth	Upstream Bandwidth	QoS Priority

1	G.Bandwidth = 128 Kbps
	M.Bandwidth = 512 Kbps
		G.Bandwidth = 64 Kbps
		M.Bandwidth = 128 Kbps
			High

Definition

Name: The name of the QoS you want to configure.

Downstream Bandwidth: To configure the Guarateed Bandwidth and Maximum Bandwidth.

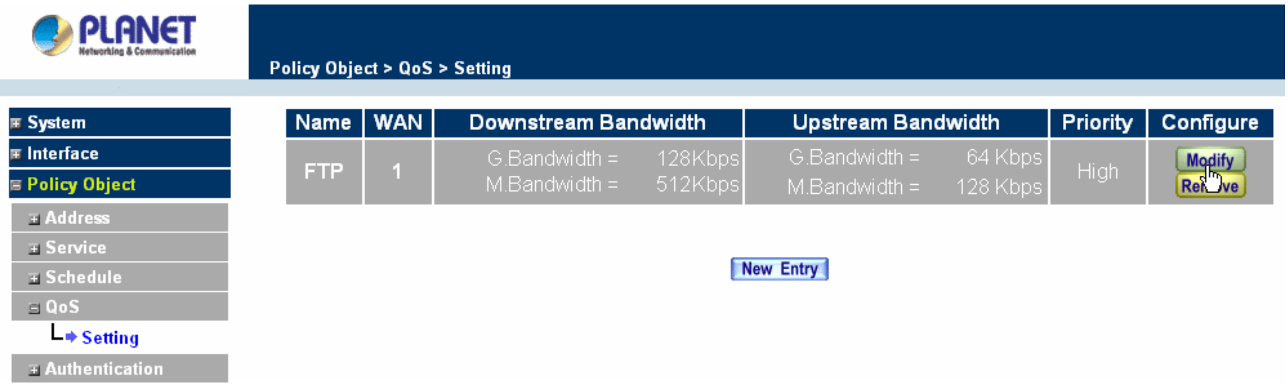
Upstream Bandwidth: To configure the Guarateed Bandwidth and Maximum Bandwidth.

QoS Priority: To configure the priority of distrubuting Upstream/Downstream and unused bandwidth.

Click the **OK** button to add new QoS.

Modify QoS

Step 1. Click QoS in the menu bar on the left hand side.



Name	WAN	Downstream Bandwidth	Upstream Bandwidth	Priority	Configure
FTP	1	G.Bandwidth = 128Kbps M.Bandwidth = 512Kbps	G.Bandwidth = 64 Kbps M.Bandwidth = 128 Kbps	High	Modify Remove

Click the Modify button to modify QoS.

Definition:

Name: The name of the QoS you want to configure.

Downstream Bandwidth: To configure the Guarateed Bandwidth and Maximum Bandwidth.

Upstream Bandwidth: To configure the Guarateed Bandwidth and Maximum Bandwidth.

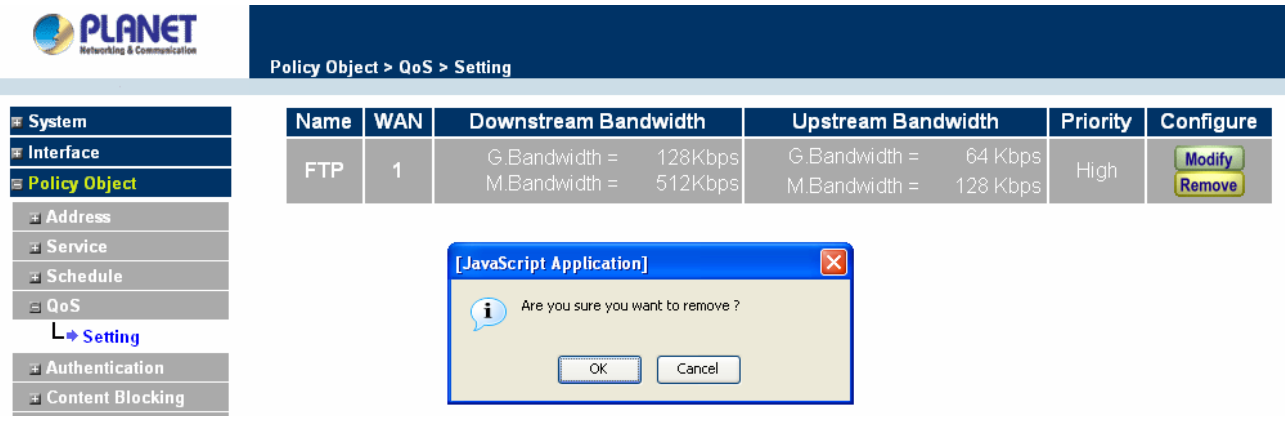
QoS Priority: To configure the priority of distrubuting Upstream/Downstream and unused bandwidth.

Click the **OK** button to modify QoS.

Delete QoS

Step 1. In the QoS window, find the QoS you want to change, and click **Delete** in the Configure column.

Step 2. In the Delete QoS window, click **OK** to delete the QoS or click Cancel to discard the change.



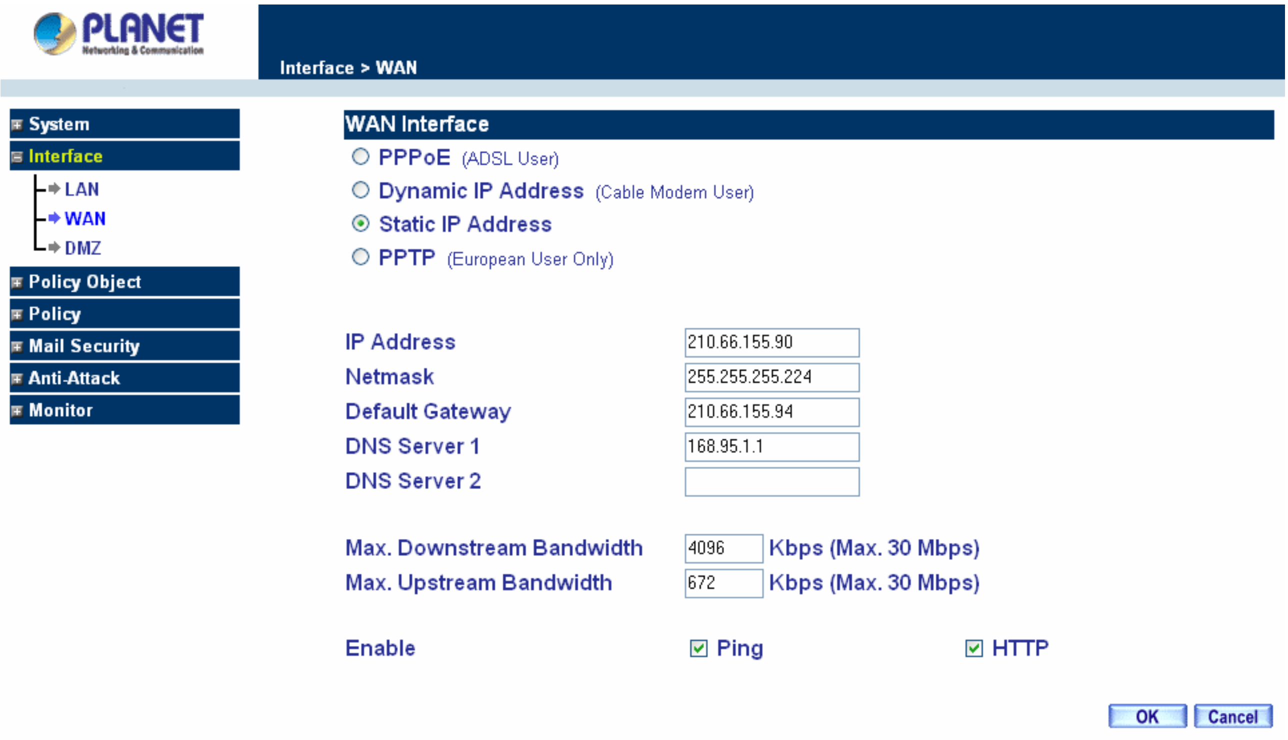
Name	WAN	Downstream Bandwidth	Upstream Bandwidth	Priority	Configure
FTP	1	G.Bandwidth = 128Kbps M.Bandwidth = 512Kbps	G.Bandwidth = 64 Kbps M.Bandwidth = 128 Kbps	High	Modify Remove

[JavaScript Application]

Are you sure you want to remove ?

Example about how to install QoS correctly

Step 1. Select and configure the correct connection type, including downstream/upstream bandwidth.



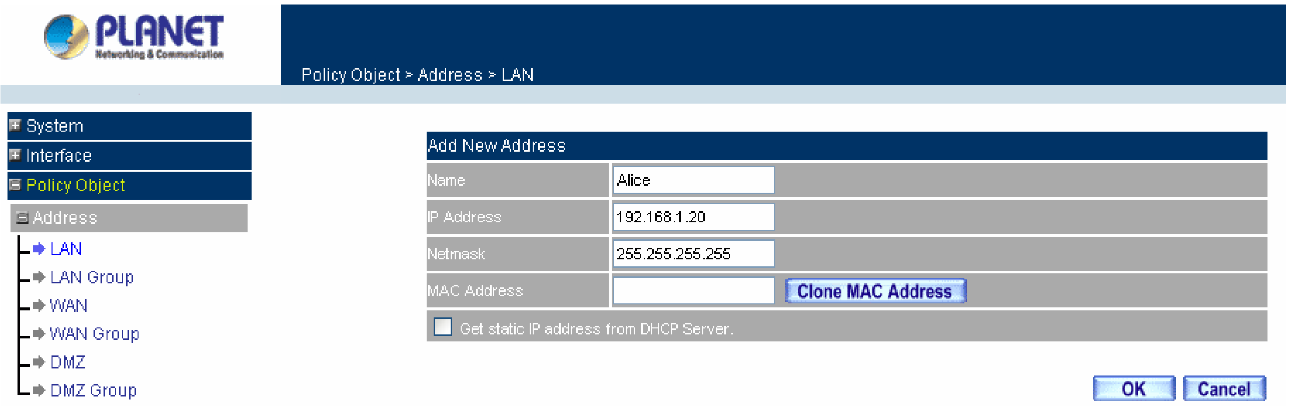
WAN Interface

○ PPPoE (ADSL User)
○ Dynamic IP Address (Cable Modem User)
● Static IP Address
○ PPTP (European User Only)

IP Address	210.66.155.90
Netmask	255.255.255.224
Default Gateway	210.66.155.94
DNS Server 1	168.95.1.1
DNS Server 2	
Max. Downstream Bandwidth	4096 Kbps (Max. 30 Mbps)
Max. Upstream Bandwidth	672 Kbps (Max. 30 Mbps)

Enable ☑ Ping ☑ HTTP

Step 2. Configure the LAN host or WAN host IP address that need to filter with QoS feature. Be aware that the Netmask must set to 255.255.255.255 if you only want to configure a single IP address.

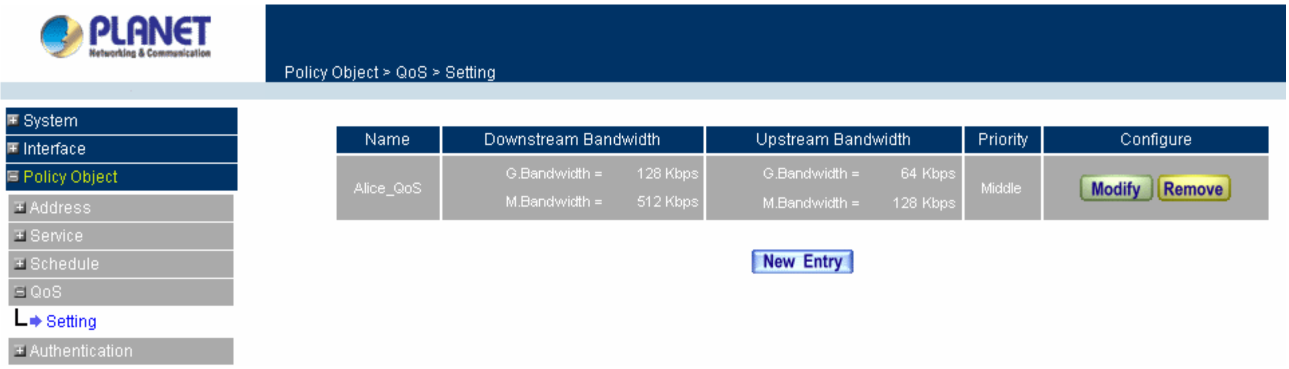


Add New Address

Name	Alice
IP Address	192.168.1.20
Netmask	255.255.255.255
MAC Address	

□ Get static IP address from DHCP Server.

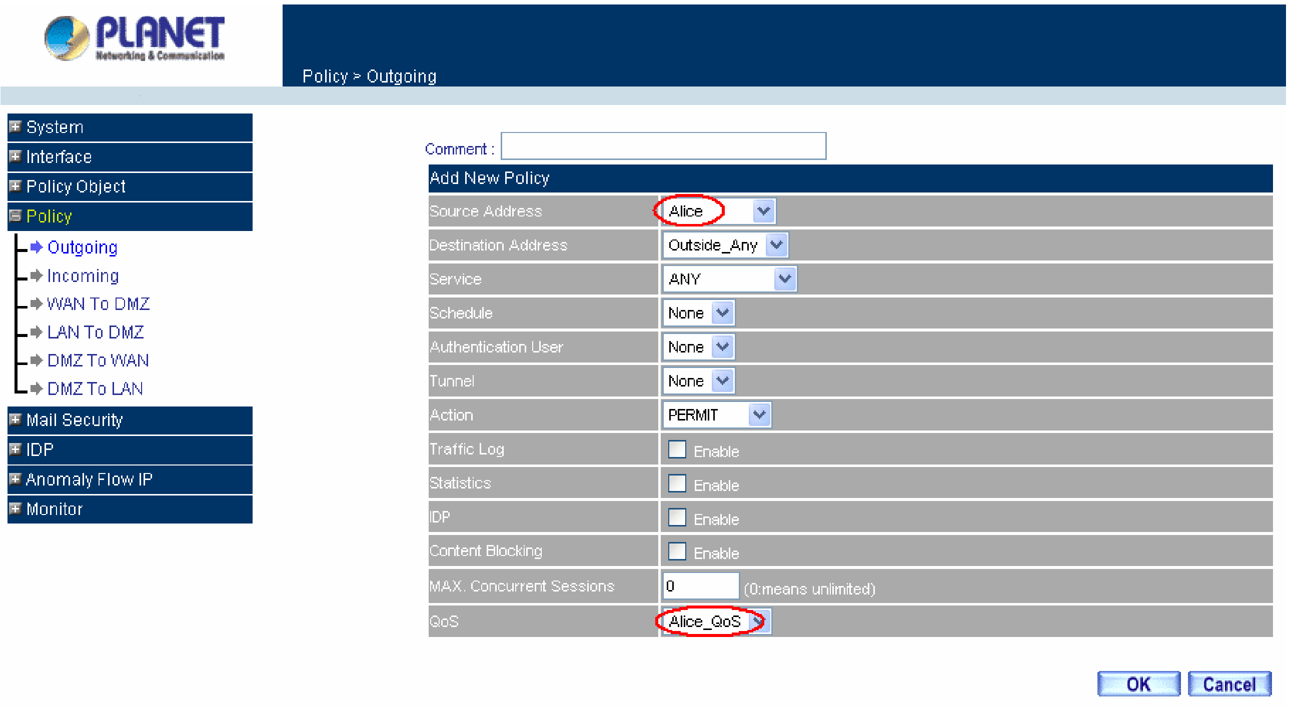
Step 3. Set up the QoS rule.



Name	Downstream Bandwidth	Upstream Bandwidth	Priority	Configure

Alice_QoS	G.Bandwidth = 128 Kbps
	M.Bandwidth = 512 Kbps
		G.Bandwidth = 64 Kbps
		M.Bandwidth = 128 Kbps
			Middle	Modify Remove

Step 4. Enable the QoS rule in Outgoing or Incoming Policy.



Comment :

Add New Policy	
Source Address	Alice
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
Tunnel	None
Action	PERMIT
Traffic Log	□ Enable
Statistics	□ Enable
IDP	□ Enable
Content Blocking	□ Enable
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	Alice_QoS

4.3.5 Authentication

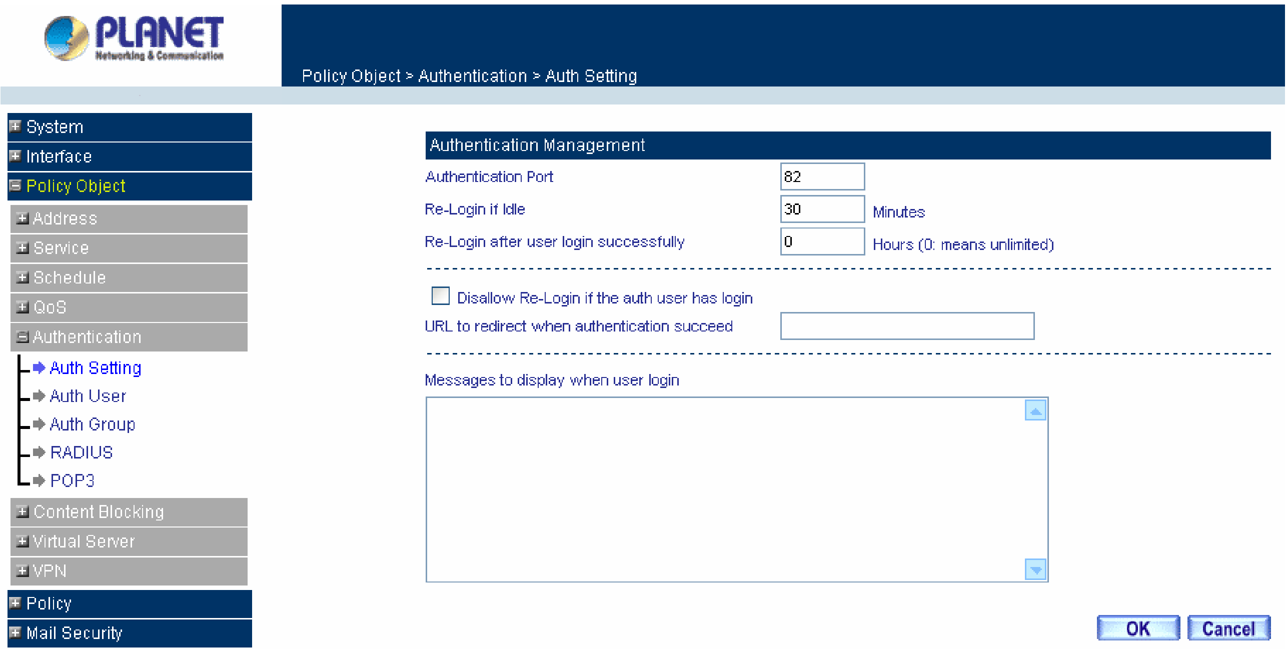
By configuring the Authentication, you can control the user's access right time of LAN to WAN. The administrator can configure the authentication according to the authentication account and password.
CS-500 configures the authentication of LAN's user by setting account and password to identify the privilege.

4.3.5.1 Auth Setting

The administrator can specify the port number and authentication time of authentication management system for LAN user to access WAN network.

Configuration of Authentication

Click **Authentication** in the menu bar on the left hand side and click **Auth Setting**.



Authentication Management

Authentication Port: 82

Re-Login if Idle: 30 Minutes

Re-Login after user login successfully: 0 Hours (0: means unlimited)

□ Disallow Re-Login if the auth user has login

URL to redirect when authentication succeed:

Messages to display when user login

Authentication Port: The port number used for user login page.

Generally, when user want to access WAN network and the authentication (Policy -> Outgoing) is enabled, the user only need to open a web page and the User Login page will pop up.

But if user does not need to open the web page and also want to access Internet resource such as FTP, then the user has to send http request with this port number, and CS-500 will send a User Login page for user to input user name and password.

For example, if the gateway IP address is 192.168.1.1 and authentication port is 82, user have to open a web browser and input http://192.168.1.1:82 on the address file to have the user login page.

Re-Login if Idle: When the LAN users access to WAN network and do not use for a while, the connection will be time-out. User has to re-login again. The default time is 30 minutes.

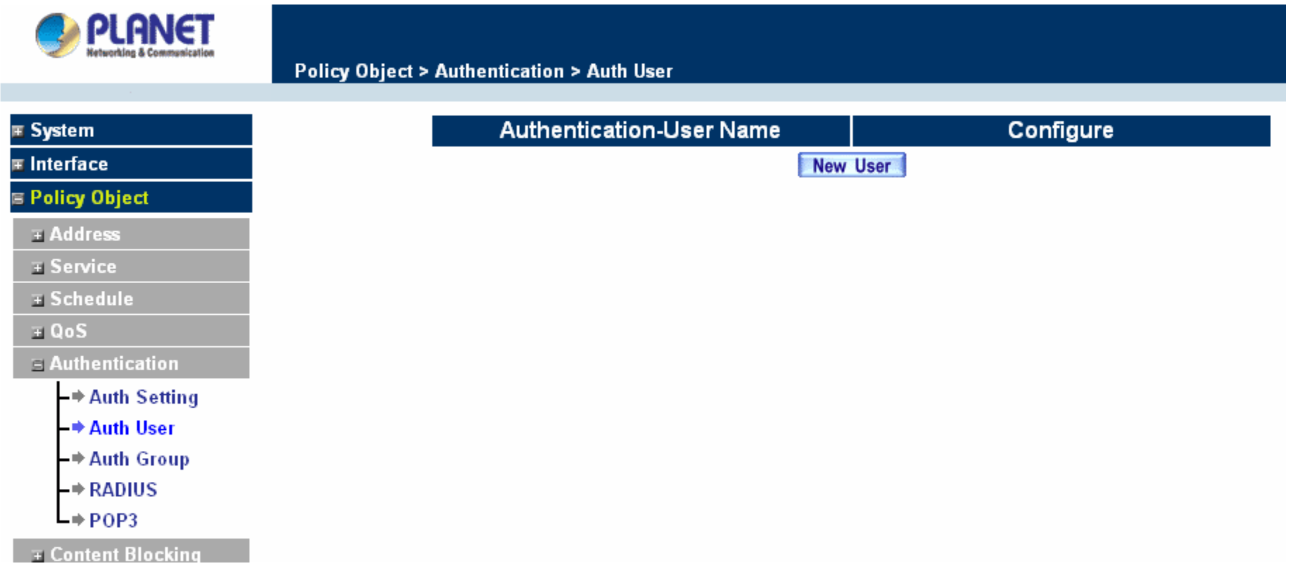
Re-Login after user login successfully: You can limit the access time for the LAN user, when time is up LAN user will need to re-login again. If the time setting sets to 0 that means unlimited. Select **Disallow Re-login if the auth user has login** will disable this feature.

URL to redirect when authentication succeed: You can set up the default webpage to force user to access it first when user passes the authentication.

Messages to display when user login: You can specify a message to display at user's login page when user passes the authentication.

4.3.5.2 Auth User

Click **Authentication** in the menu bar on the left hand side and click **Auth User**.



Definitions:

Name：The name of the Authentication you want to configure.

Configure: modify settings or remove users.

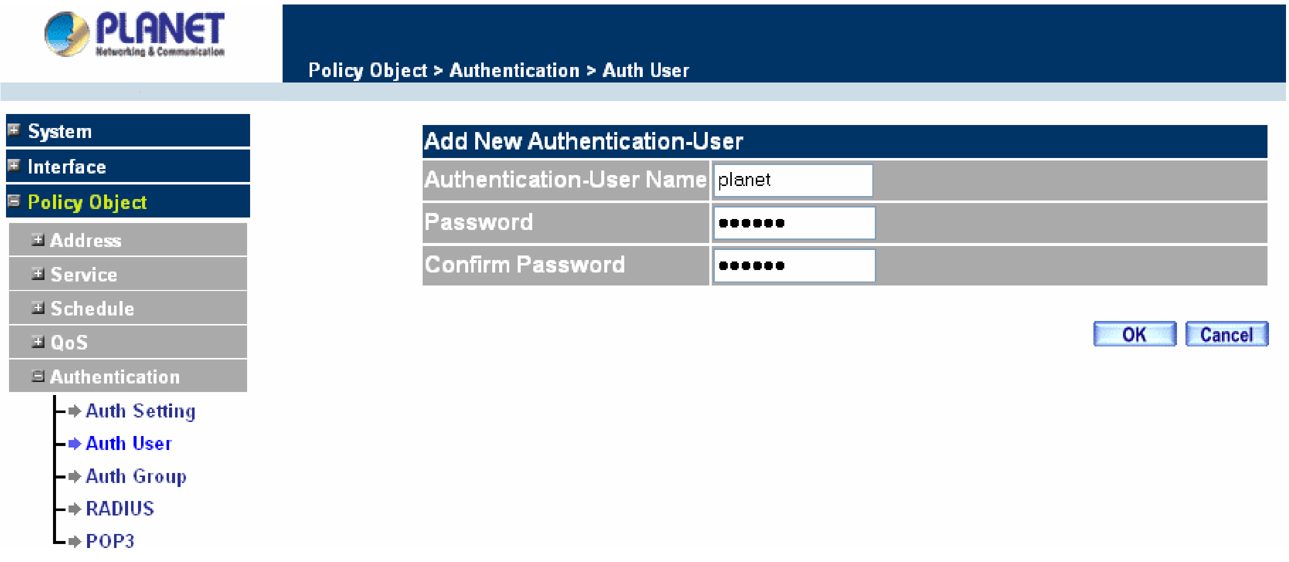
Adding a new Auth User

Step 1. In the **Authentication** window, click the **New User** button to create a new **Auth User.**

Step 2. In the **Auth-User** window:

- **Auth-User Name:** enter the username of new **Authentication.**
- **Password:** enter a password for the new **Authentication.**
- **Confirm Password:** enter the password again.

Step 3. Click **OK** to add the user or click **Cancel** to cancel the addition.

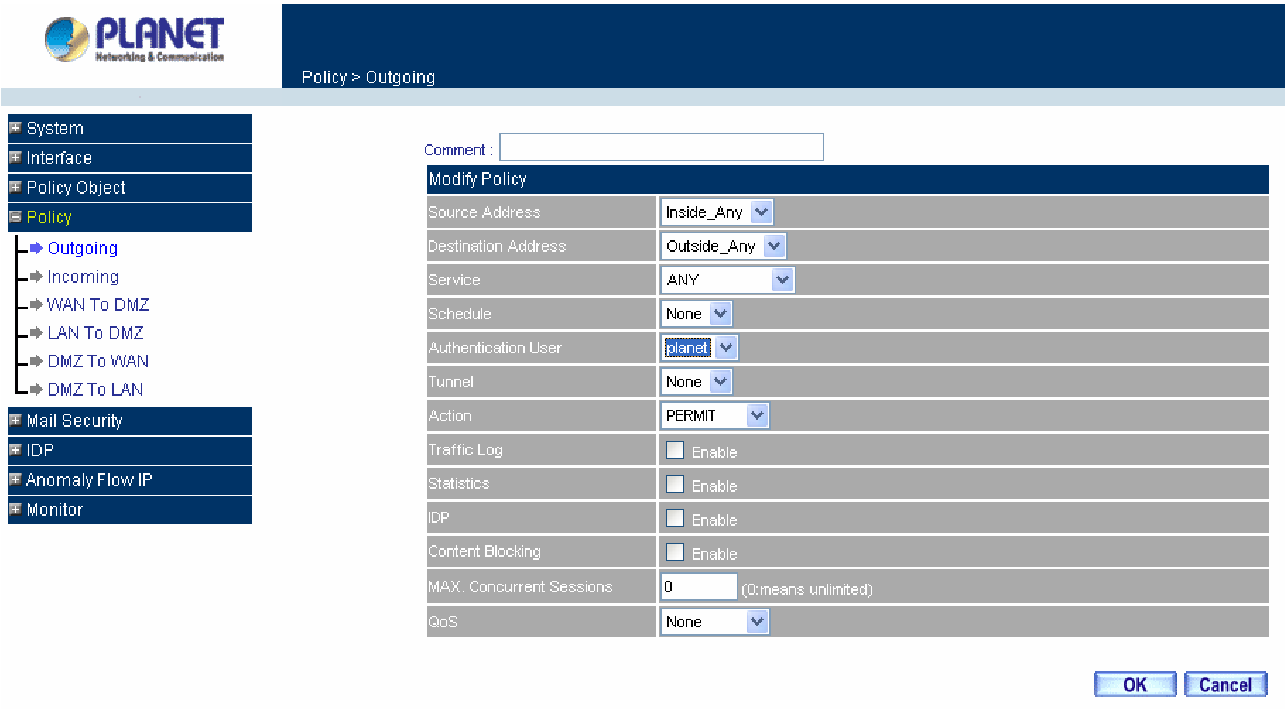


Add New Authentication-User

Authentication-User Name	planet
Password	••••••
Confirm Password	••••••

NOTE: When the LAN user access to WAN network and do not use for a while, the connection will be time-out. User has to re-login again. The default time is 30 minutes and you can configure this time by "Authentication"-> "Auth Setting" page.

In the form of controlling the [Outgoing] Policy, enable the Authentication-User Function.

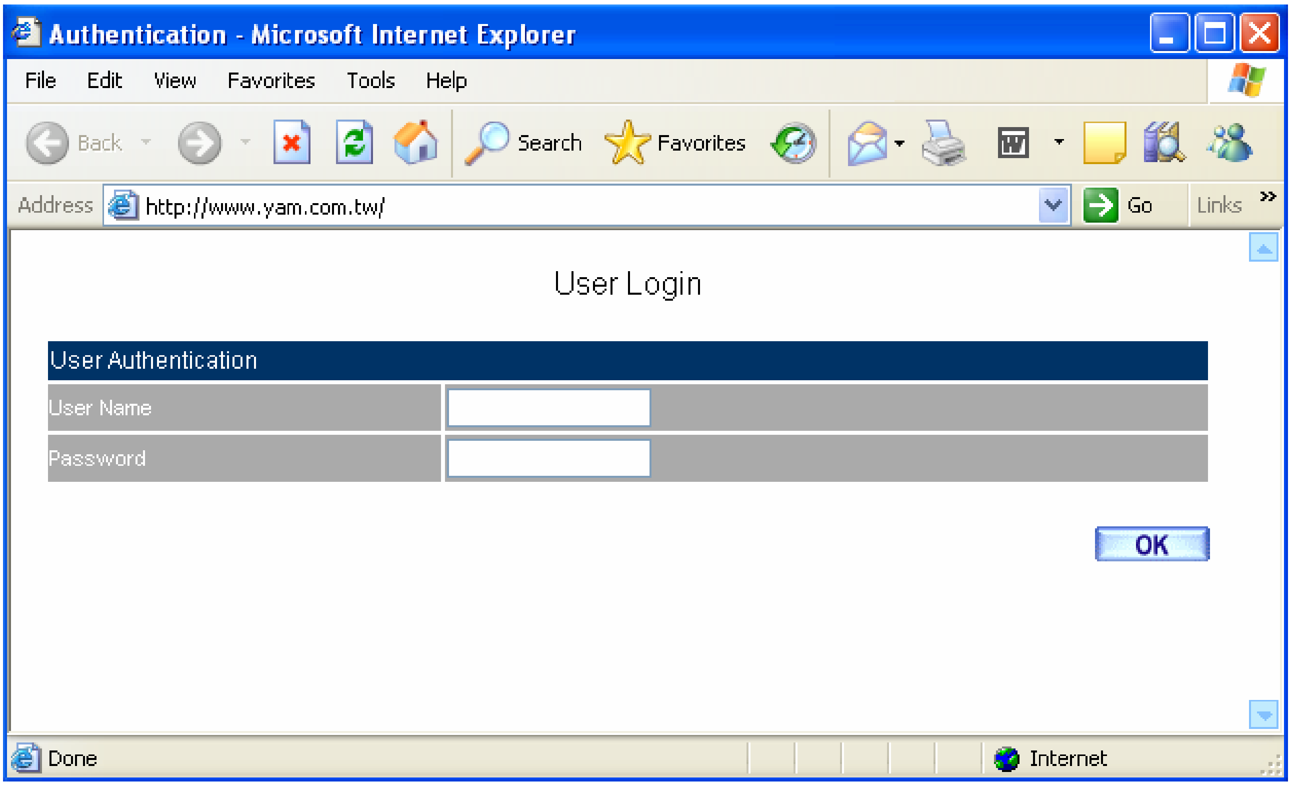


Comment :

Modify Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	planet
Tunnel	None
Action	PERMIT
Traffic Log	□ Enable
Statistics	□ Enable
IDP	□ Enable
Content Blocking	□ Enable
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None

User Login Page Definitions:

- **User Name**: The name of the Authentication you want to configure.
- **Password**: The input carries on the authentication the password


Authentication - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.yam.com.tw/
Go Links
OK
Done
Internet

User Login

User Authentication	
User Name	
Password	

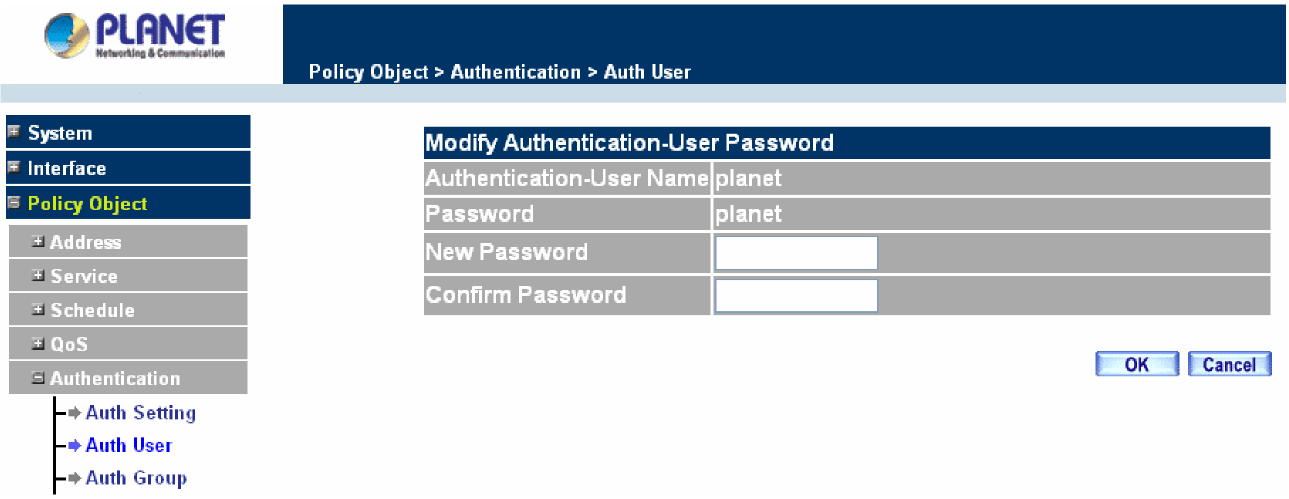
Modifying the Authentication User

Step 1. In the **Authentication** window, locate the **Auth-User** name you want to edit, and click on **Modify** in the **Configure** field.

Step 2. The **Modify Auth-User Password** window will appear. Enter in the required information:

- **Auth-User:** show original authentication user.
- **Password:** show original password.
- **New Password:** enter new password
- **Confirm Password:** enter the new password again.

Step 3. Click **OK** to confirm authentication user change or click **Cancel** to cancel it.



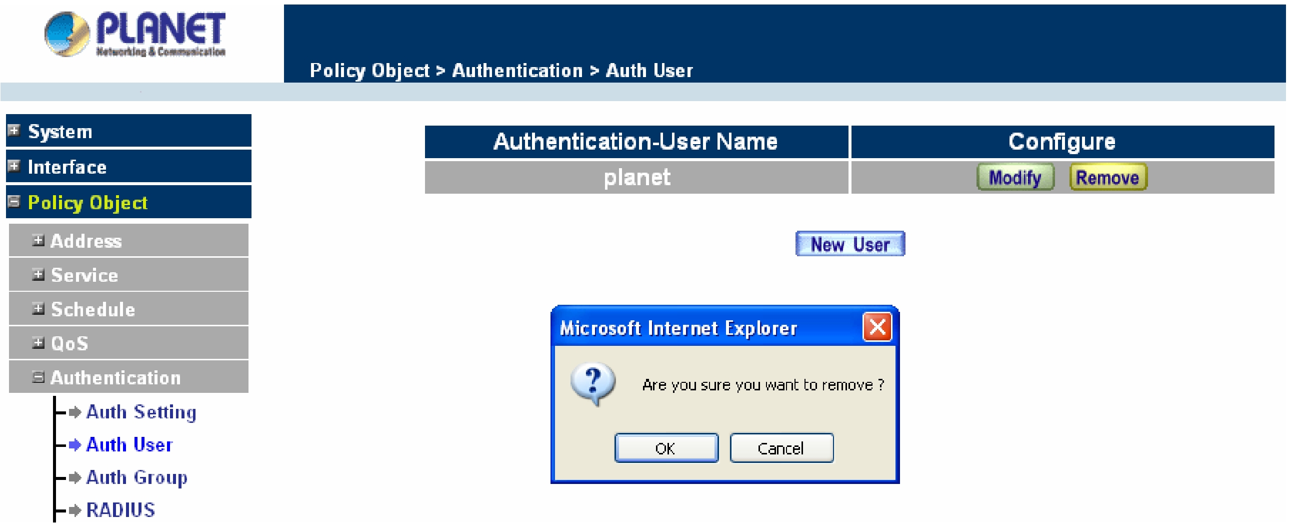
Modify Authentication-User Password	
Authentication-User Name	planet
Password	planet
New Password	
Confirm Password	

Removing a Authentication User

Step 1. In the Authentication table, locate the Auth-User name you want to edit, and click on the Remove option in the Configure field.

Step 2. The Remove confirmation pop-up box will appear.

Step 3. Click **OK** to remove that Authentication User or click **Cancel** to cancel.



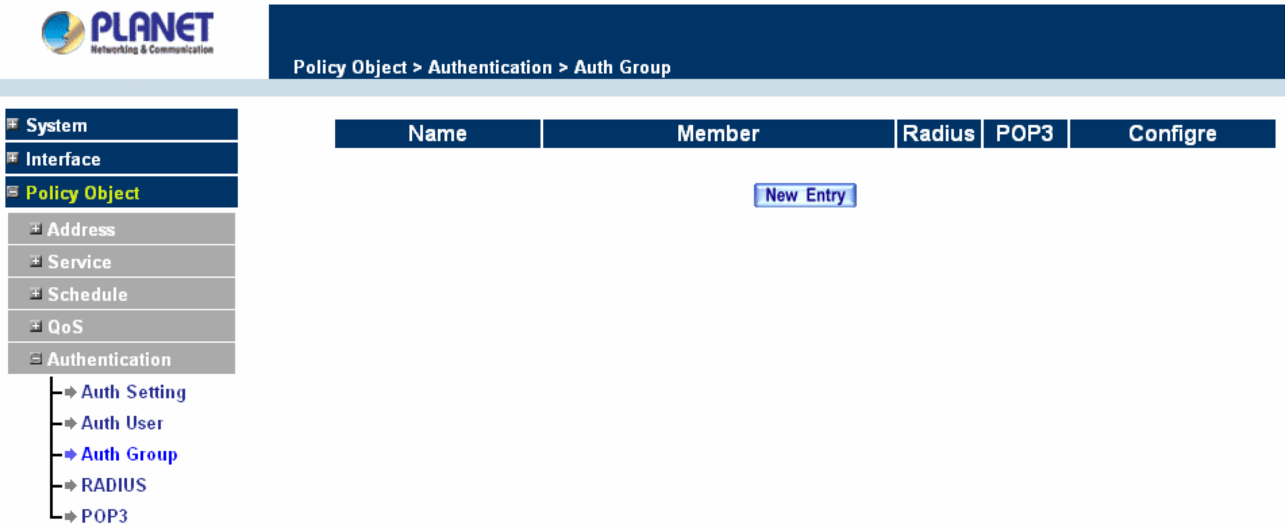
Authentication-User Name	Configure
planet	Modify Remove

Are you sure you want to remove ?

4.3.5.3 Auth Group

Accessing the Auth Group window

Click **Authentication** in the menu bar on the left hand side of the window. Click **Auth Group** under it. A window will appear with a table displaying current Auth Group settings by the Administrator.



Name	Member	Radius	POP3	Configre

Adding Auth Group

Step 1. In the Auth Group window, click the **New Entry** button.

In the Auth Group window, the following fields will appear:

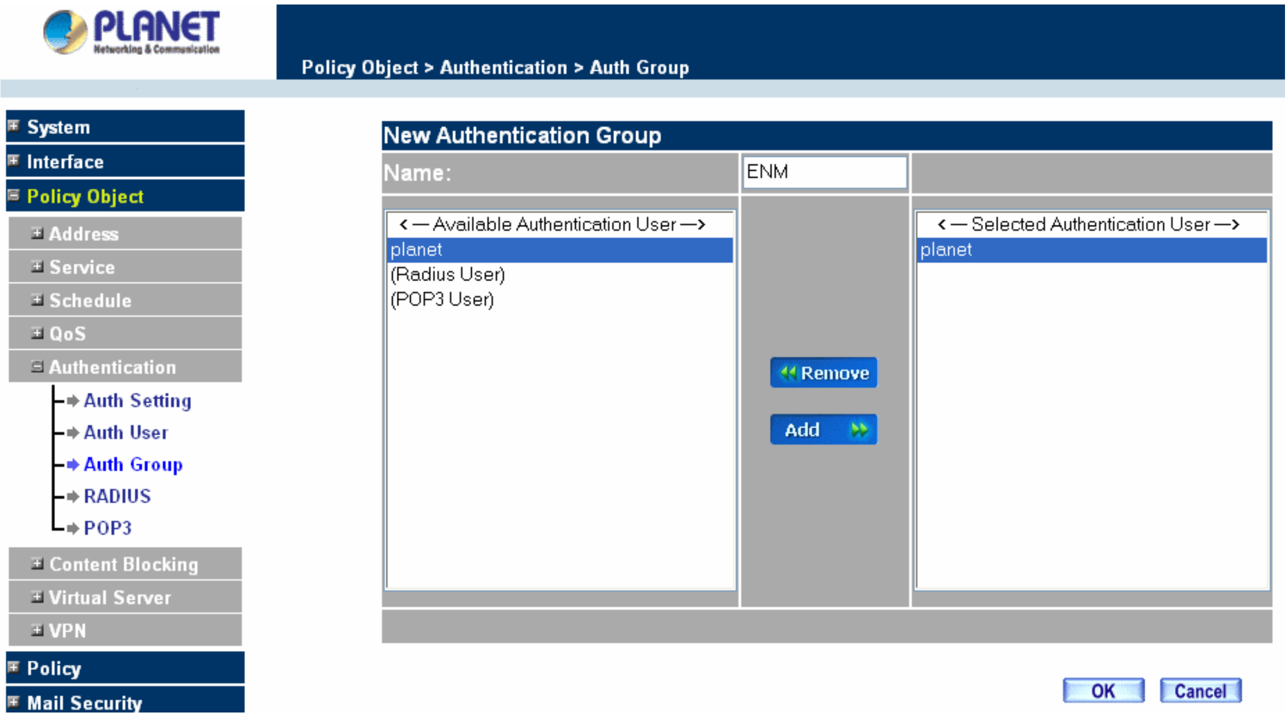
- **Name:** Enter the new Auth Group name.
- **Available auth user:** List all the available Auth User.
- **Selected auth user:** List Auth User to be assigned to the new group.

Step 2. Enter the new group name in the group **Name** field. This will be the name referencing the created group.

Step 3. **To add new Auth User:** Select the Auth User desired to be added in the **Available auth user** list, and then click the **Add>>** button to add them to the group.

Step 4. **To remove Auth User:** Select Auth User desired to be removed in the **Available auth user** list, and then click the **<<Remove** button to remove them from the group.

Step 5. Click **OK** to add the new group.



Name: ENM

<—Available Authentication User—>
planet
(Radius User)
(POP3 User)

<—Selected Authentication User—>
planet

Modifying Auth Group

Step 1. In the Auth Group window, locate the Auth Group to be edited. Click its corresponding **Modify** option in the **Configure** field.

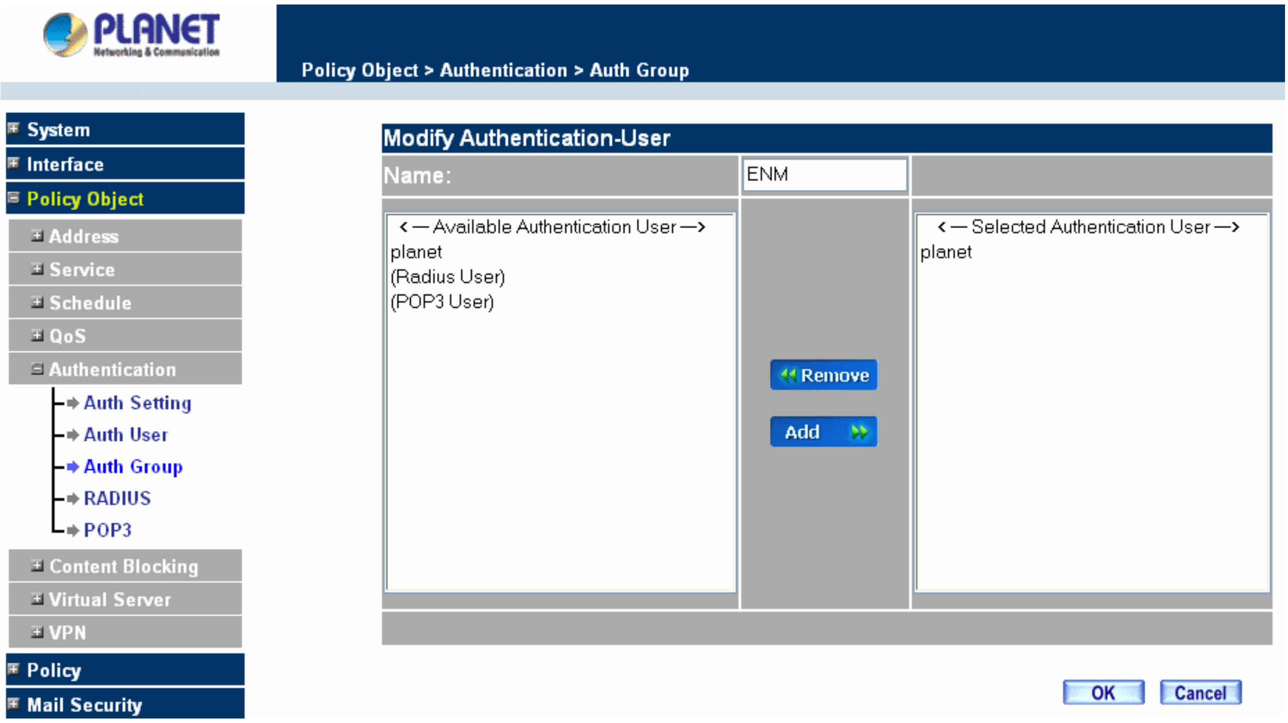
Step 2. In the **Modify Auth group** window the following fields are displayed::

- **Name:** Enter the new Auth Group name .
- **Available auth user:** List all the available Auth User.
- **Selected auth user:** List Auth User to be assigned to the new group.

Step 3. **To add new Auth User:** Select the Auth User desired to be added to the **Available auth user** list, and then click the **Add>>** button to add them to the group.

Step 4. **To remove Auth User:** Select Auth User desired to be removed from the **Available auth user** list, and then click the **<<Remove** button to remove them from the group.

Step 5. Click **OK** to modify the Group.



Modify Authentication-User

Name: ENM

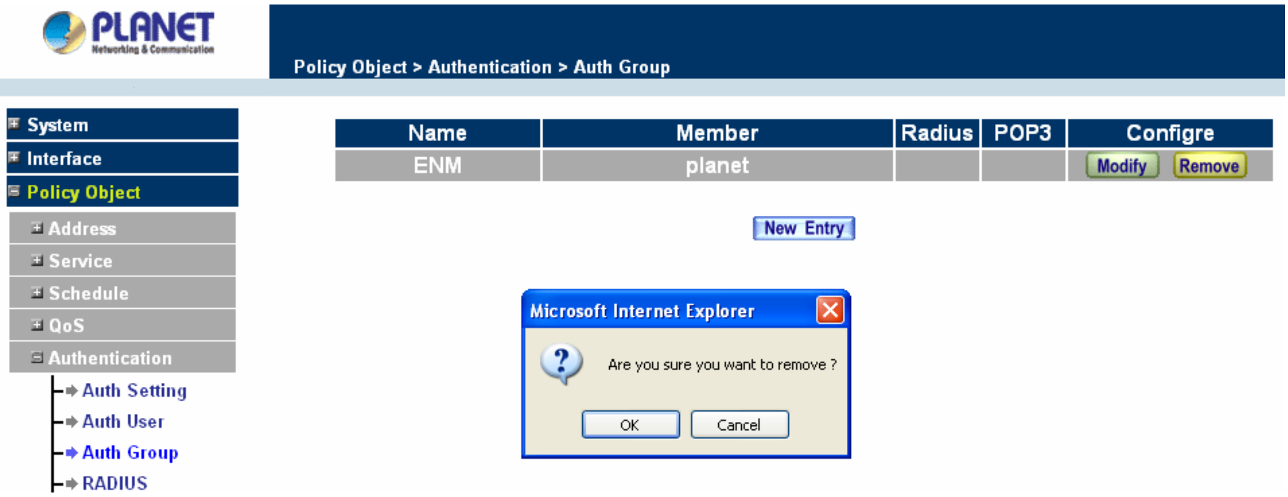
<—Available Authentication User—>
planet
(Radius User)
(POP3 User)

<—Selected Authentication User—>
planet

Removing Auth Group

Step 1. In the **Auth Group** window, locate the Auth Group to be removed and click its corresponding **Remove** option in the **Configure** field.

Step 2. In the **Remove** confirmation pop-up box, click **OK** to remove the selected service group or click **Cancel** to cancel removing.

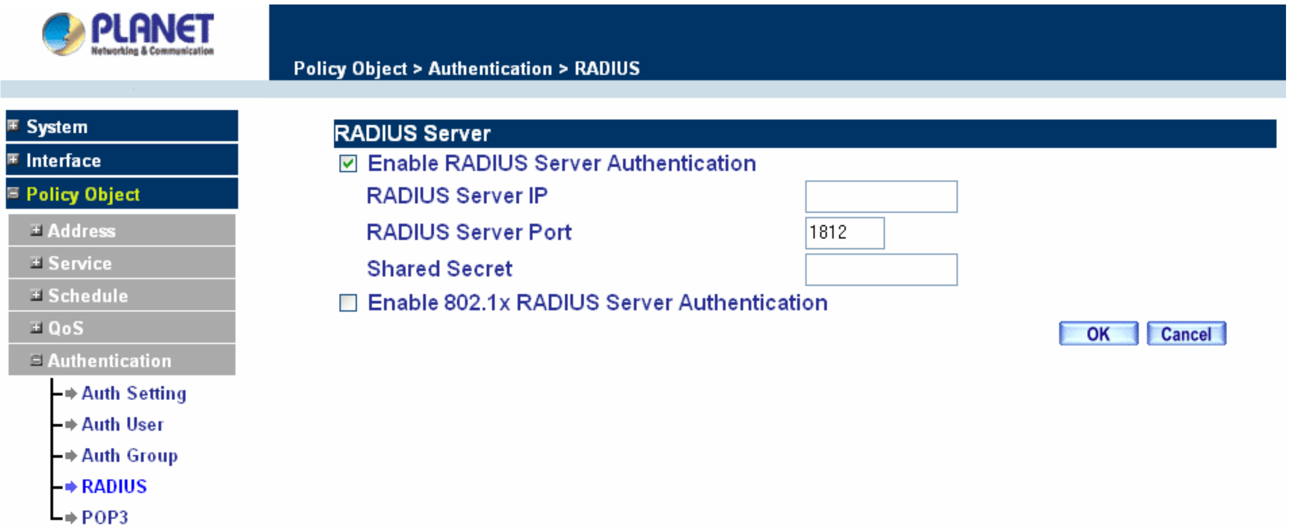


Name	Member	Radius	POP3	Configre
ENM	planet			Modify Remove

Are you sure you want to remove ?

4.3.5.4 Radius Serve

Click **Authentication** on the left side menu bar, then click **Radius Server** below it. The following window is shown.



Policy Object > Authentication > RADIUS

RADIUS Server

☑ Enable RADIUS Server Authentication

RADIUS Server IP:

RADIUS Server Port: 1812

Shared Secret:

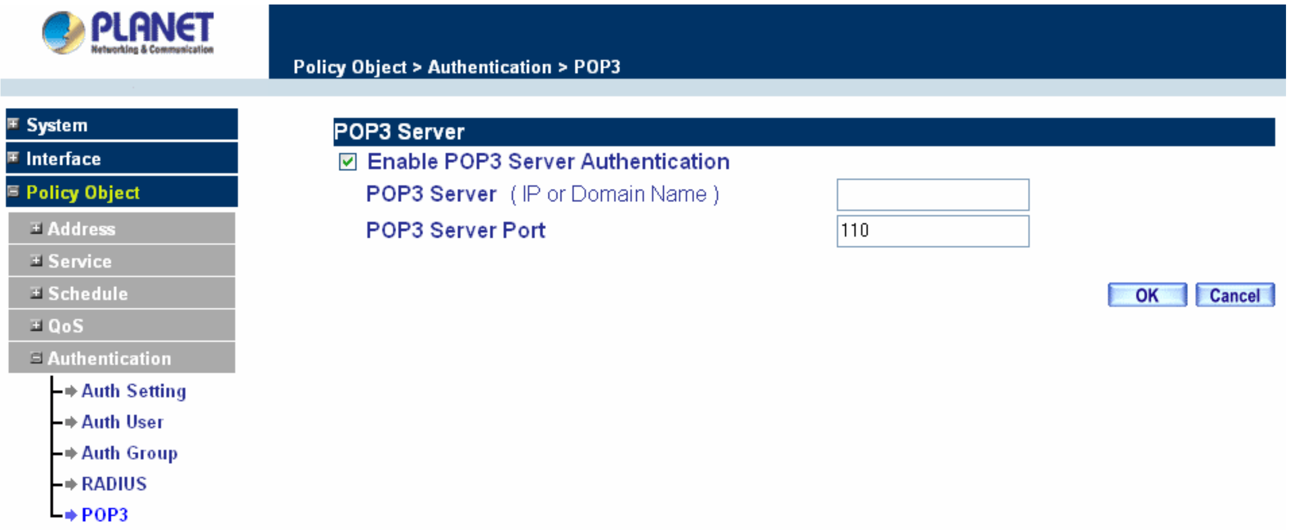
□ Enable 802.1x RADIUS Server Authentication

Definition

- **Enable RADIUS Server**: Enable RADIUS Server Authentication.
- **RADIUS Server IP**: Enter RADIUS Server IP address.
- **RADIUS Server Port**: Enter RADIUS Server Port. The default port is 1812.
- **Shared Secret**: The Password for CS-500 to access RADIUS Server.
- **Enable 802.1x RADIUS Server Authentication**: Enable 802.1x RADIUS Server Authentication.

4.3.5.5 POP3

Click **Authentication** on the left side menu bar, then click **POP3** below it. The following window is shown.



Policy Object > Authentication > POP3

POP3 Server

☑ Enable POP3 Server Authentication

POP3 Server (IP or Domain Name):

POP3 Server Port: 110

Definition

- **Enable POP3 Server**: Enable POP3 Server Authentication.
- **POP3 Server** : Enter POP3 Server IP address or domain name.
- **POP3 Server Port**: Enter POP3 Server Port. The default port is 110.

4.3.6 Content Blocking

Content Blocking includes “**URL**”, “**Scripts**”, “**P2P**”, “**IM**”, “**Download**” and “**Upload**”.

URL: The administrator can use a complete domain name or key word to make rules for specific websites.

Scripts : To let Popup、ActiveX、Java、Cookie in or keep them out.

P2P : Block P2P program, include “eDonkey”, “Bit Torrent“ and “WinMX”.

IM : Block Internet Message program, include “MSN”, “Yahoo Messenger”, “ICQ”, “QQ” and “Skype”.

Download : Block download connection, audio and video transferring from web page. You can select to block which type of extension name or all type of the file.

Upload : Block upload connection, audio and video transferring from web page. You can select to block which type of extension name or all type of the file.

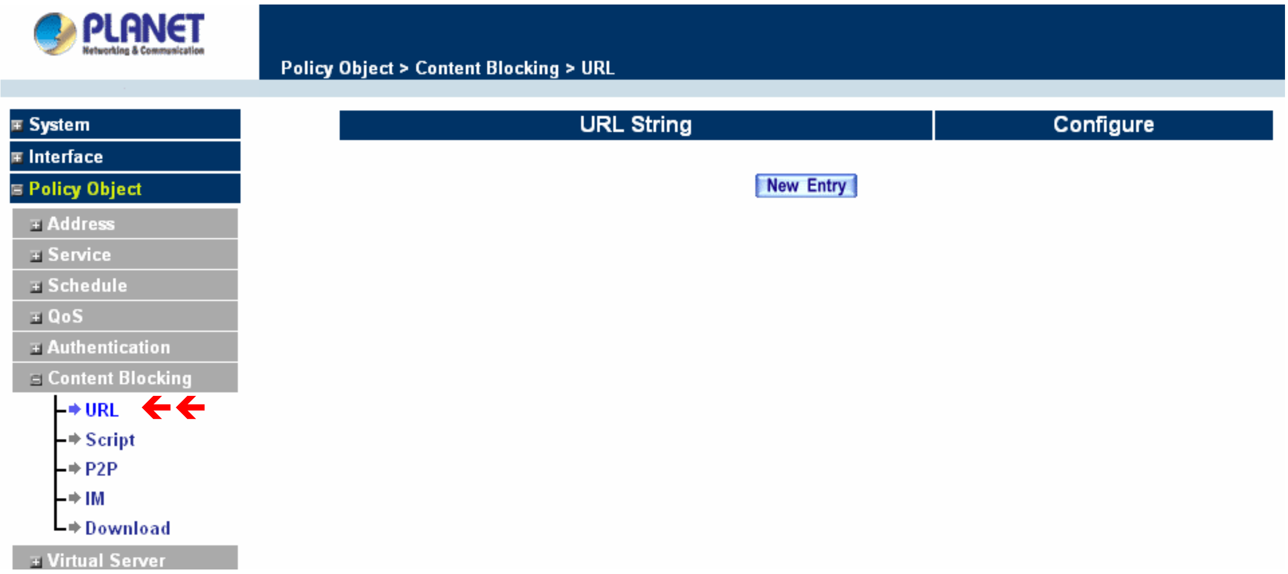
4.3.6.1 URL Blocking

The Administrator may setup URL Blocking to prevent LAN network users from accessing a specific website on the Internet. Any web request coming from an LAN network computer to a blocked website will receive a blocked message instead of the website.

Entering the URL blocking window

Step 1. Click on **URL** under the **Content Blocking** menu bar.

Step 2. Click on **New Entry.**



Definition:

URL String: The domain name that is blocked to enter by Content Security Gateway.

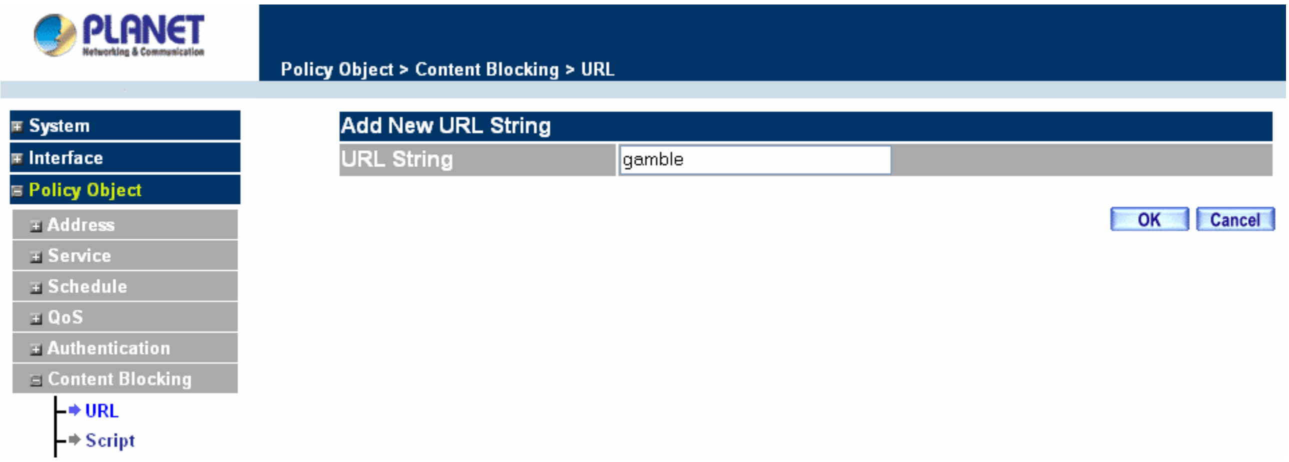
Configure: To change the settings of URL Blocking, click **Modify** to change the parameters; click **Delete** to delete the settings.

Adding a URL policy

Step 1. After clicking **New Entry**, the **Add New URL String** window will appear.

Step 2. Enter the URL of the website to be blocked.

Step 3. Click **OK** to add the policy. Click **Cancel** to discard changes.



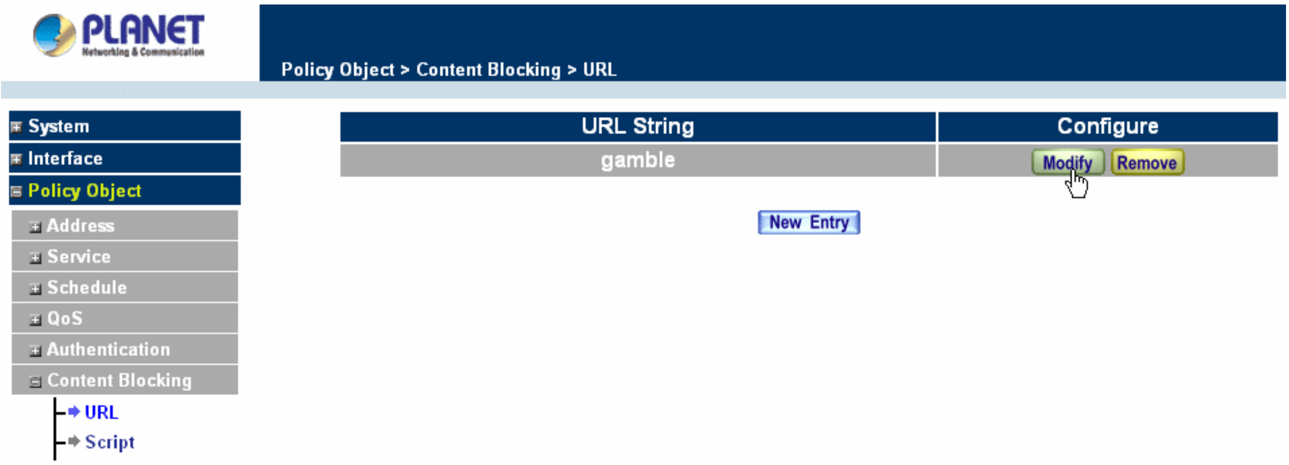
URL String	gamble

Modifying a URL String Policy

Step 1. In the **URL** window, find the policy to be modified and click the corresponding **Modify** option in the **Configure** field.

Step 2. Make the necessary changes needed.

Step 3. Click on **OK** to save changes or click on **Cancel** to discard changes.

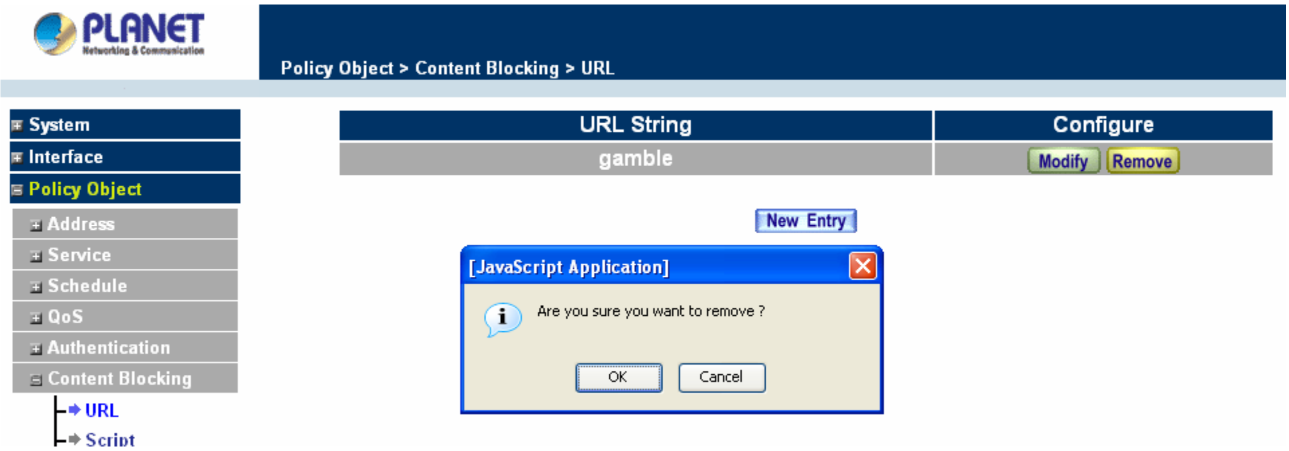


URL String	Configure
gamble	Modify Remove

Removing a URL String policy

Step 1. In the **URL** window, find the policy to be removed and click the corresponding **Remove** option in the **Configure** field.

Step 2. A confirmation pop-up box will appear, click on **OK** to remove the policy or click on **Cancel** to discard changes.



URL String	Configure
gamble	Modify Remove

Are you sure you want to remove ?

4.3.6.2 Scripts

To let Popup, ActiveX, Java, or Cookies in or keep them out.

Step 1: Click **Scripts** below **Content Blocking** menu.

Step 2: Select **Scripts** detective functions:

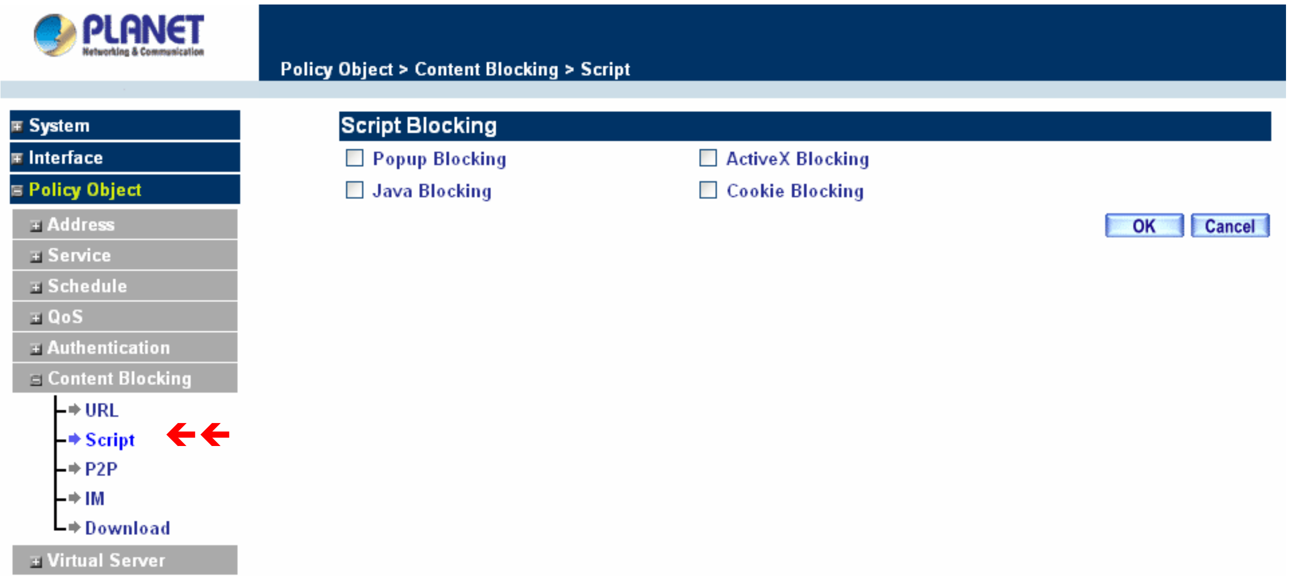
Popup Blocking: Prevent pop-up boxes from appearing.

ActiveX Blocking: Prevent ActiveX packets.

Java Blocking: Prevent Java packets.

Cookie Blocking: Prevent Cookie packets.

Step 3: After selecting each function, click the **OK** button below.



Policy Object > Content Blocking > Script

Script Blocking

☐ Popup Blocking ☐ ActiveX Blocking
☐ Java Blocking ☐ Cookie Blocking

When the system detects the setting, the Content Security Gateway will spontaneously work**.**

4.3.6.3 P2P

Step 1: Click **P2P** below **Content Blocking** menu.

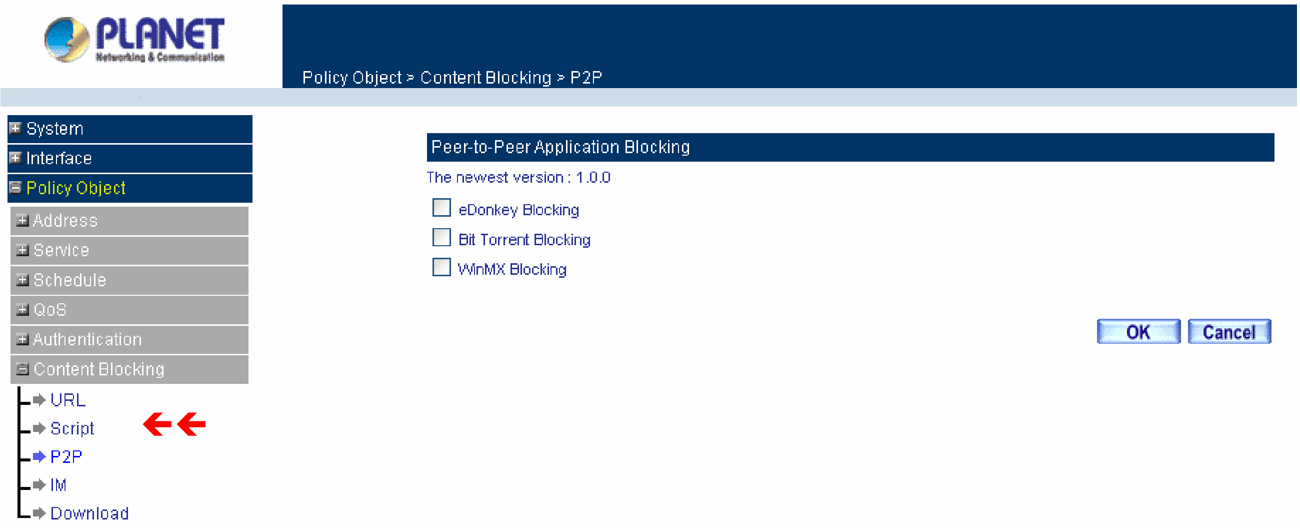
Step 2: Select **P2P** detective functions:

eDonkey Blocking: Prevent eDonkey connection built up.

Bit Torrent Blocking: Prevent Bit Torrent connection built up.

WinMX Blocking: Prevent WinMX connection built up.

Step 3: After selecting each function, click the **OK** button below.



Policy Object > Content Blocking > P2P

Peer-to-Peer Application Blocking

The newest version : 1.0.0

☐ eDonkey Blocking
☐ Bit Torrent Blocking
☐ WinMX Blocking

CS-500 provides a feature that will auto detect the P2P program version. When it detects a new version P2P program in the LAN site, CS-500 will connect to Internet and download the pattern to update the P2P Blocking function, and to keep the function working well to block new version P2P program. The current pattern version will display at the top side.

4.3.6.4 IM

Step 1: Click **IM** below **Content Blocking** menu.

Step 2: Select **IM** detective functions:

MSN Messenger Blocking: To select to block MSN Messenger **login**, **File Transfer**, **Voice** or **Camera** transferring.

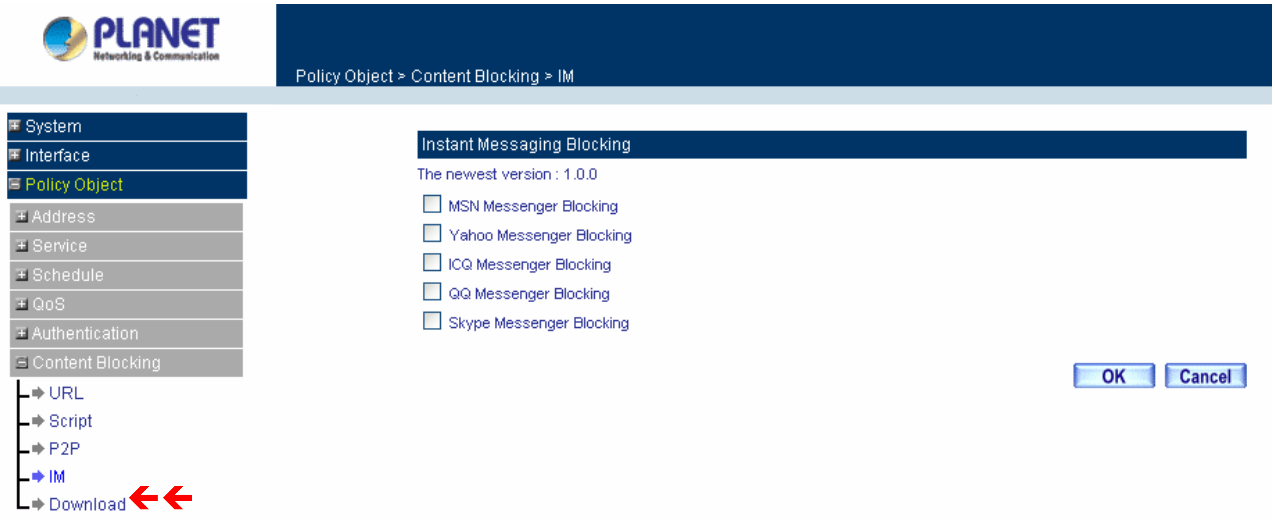
Yahoo Messenger Blocking: To select to block Yahoo Messenger **login**, **File Transfer**, **Voice** or **Camera** transferring.

ICQ Blocking: Only to select to block ICQ **login**.

QQ Blocking: Only to select to block ICQ **login**.

Skype Messenger Blocking: To select to block Skype Messenger **login**, **File Transfer**, **Voice** or **Camera** transferring.

Step 3: After selecting each function, click the **OK** button below.



Instant Messaging Blocking

The newest version : 1.0.0

□ MSN Messenger Blocking

□ Yahoo Messenger Blocking

□ ICQ Messenger Blocking

□ QQ Messenger Blocking

□ Skype Messenger Blocking

CS-500 provides a feature that will auto detect the IM program version. When it detects a new version IM program in the LAN site, CS-500 will connect to Internet and download the pattern to update the IM Blocking function, and to keep the function working well to block new version IM program. The current pattern version will display at the top side.

4.3.6.5 Download

Step 1: Click **Download** below **Content Blocking** menu.

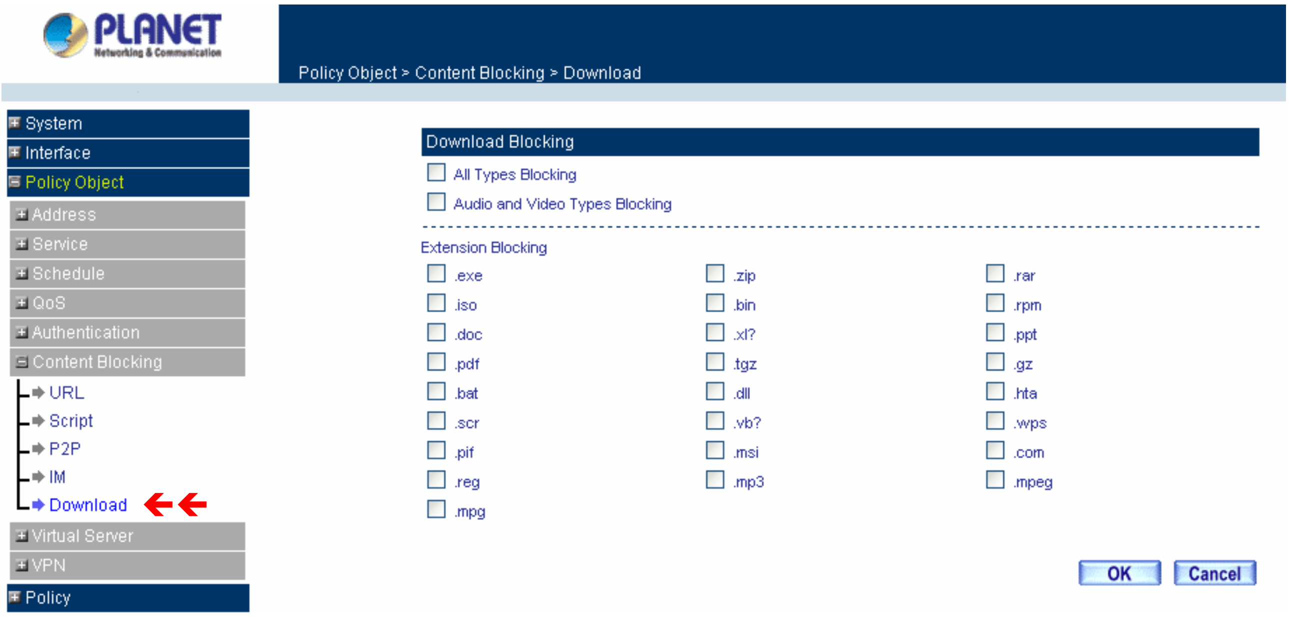
Step 2: Select **Download** detective functions:

All Types Block: To block all types of the files downloading from web page.

Audio and Video Types block: To block audio and video downloading from web page..

Extensions Block: To block specific extensions name of the files from web page.

Step 3: After selecting each function, click the **OK** button below.



Download Blocking

□ All Types Blocking

□ Audio and Video Types Blocking

Extension Blocking

□ .exe	□ .zip	□ .rar
□ .iso	□ .bin	□ .rpm
□ .doc	□ .xl?	□ .ppt
□ .pdf	□ .tgz	□ .gz
□ .bat	□ .dll	□ .hta
□ .scr	□ .vb?	□ .wps
□ .pif	□ .msi	□ .com
□ .reg	□ .mp3	□ .mpeg
□ .mpg		

4.3.6.6 Upload

Step 1: Click **Upload** below **Content Blocking** menu.

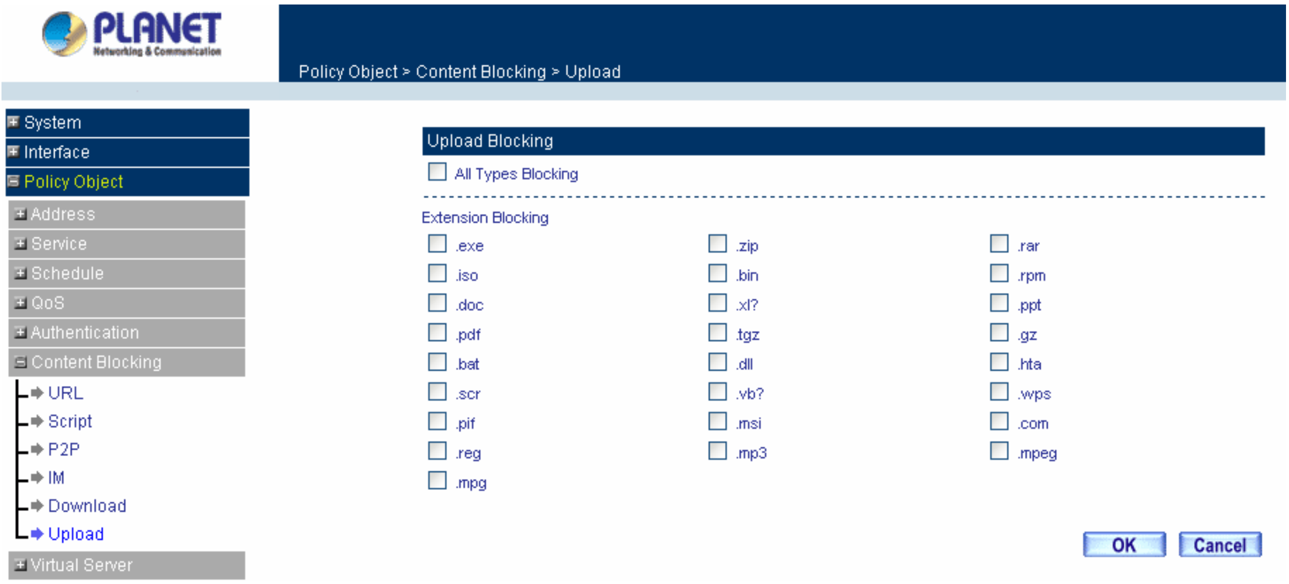
Step 2: Select **Upload** detective functions:

All Types Block: To block all types of the files uploading from web page.

Audio and Video Types block: To block audio and video uploading from web page..

Extensions Block: To block specific extensions name of the files from web page.

Step 3: After selecting each function, click the **OK** button below.



Upload Blocking

□ All Types Blocking

Extension Blocking

□ .exe	□ .zip	□ .rar
□ .iso	□ .bin	□ .rpm
□ .doc	□ .xl?	□ .ppt
□ .pdf	□ .tgz	□ .gz
□ .bat	□ .dll	□ .hta
□ .scr	□ .vb?	□ .wps
□ .pif	□ .msi	□ .com
□ .reg	□ .mp3	□ .mpeg
□ .mpg		

4.3.7 Virtual Server

The Content Security Gateway separates an enterprise's Intranet and Internet into LAN networks and WAN networks respectively. Generally, in order to allocate enough IP addresses for all computers, an enterprise assigns each computer a private IP address, and converts it into a real IP address through Content Security Gateway's NAT (Network Address Translation) function. If a server providing service to the WAN networks is located in the LAN networks, outside users can't directly connect to the server by using the server's private IP address.

The Content Security Gateway's Virtual Server can solve this problem. A virtual server has set the real IP address of the Content Security Gateway's WAN network interface to be the Virtual Server IP. Through the virtual server feature, the Content Security Gateway translates the virtual server's IP address into the private IP address of physical server in the LAN network. When outside users on the Internet request connections to the virtual server, the request will be forwarded to the private LAN server.

Virtual Server owns another feature known as one-to-many mapping. This is when one virtual server IP address on the WAN interface can be mapped into 4 LAN network server private IP addresses. This option is useful for Load Balancing, which causes the virtual server to distribute data packets to each private IP addresses (which are the real servers). By sending all data packets to all similar servers, this increases the server's efficiency, reduces risks of server crashes, and enhances servers' stability.

How to use Virtual Server and mapped IP

Virtual Server and Mapped IP are part of the IP mapping (also called DMZ, De-Militarization Zone) scheme. By applying the incoming policies, Virtual Server and IP mapping work similarly. They map real IP addresses to the physical servers' private IP addresses (which are opposite to NAT), but there are still some differences:

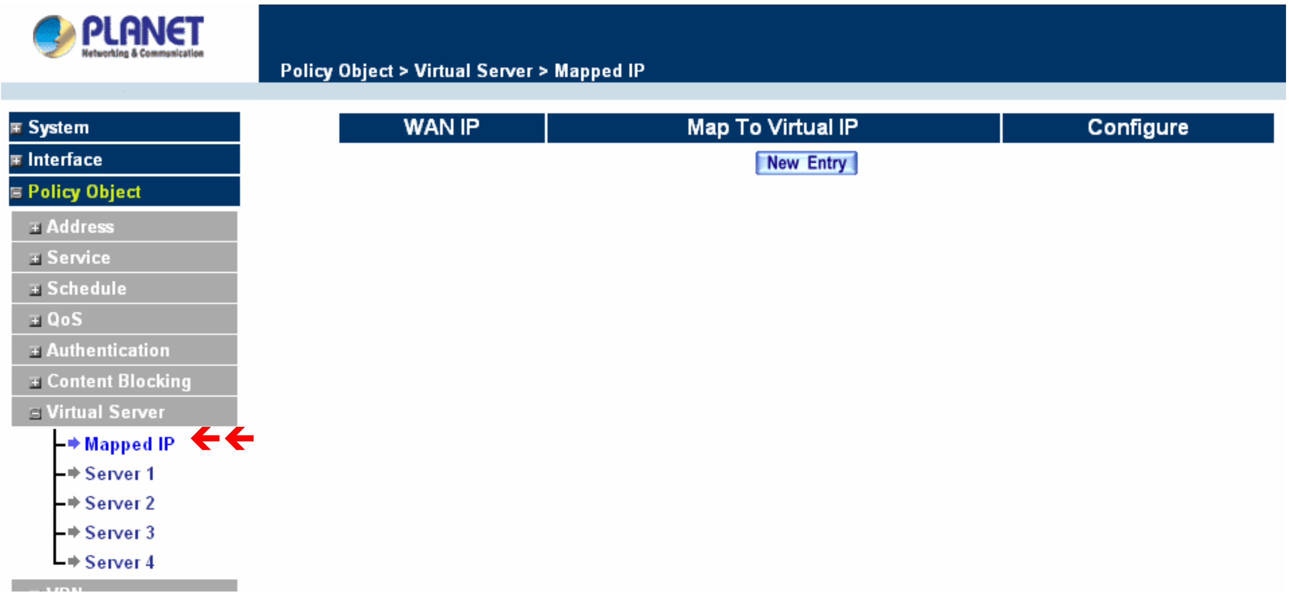
- Virtual Server can map one real IP to several LAN physical servers while Mapped IP can only map one real IP to one LAN physical server (1-to-1 Mapping). The Virtual Servers' load balance feature can map a specific service request to different physical servers running the same services.
- Virtual Server can only map one real IP to one service/port of the LAN physical servers while Mapped IP maps one real IP to all the services offered by the physical server.
- IP mapping and Virtual Server work by binding the IP address of the WAN virtual server to the private LAN IP address of the physical server that supports the services. Therefore users from the WAN network can access servers of the LAN network by requesting the service from the IP address provided by Virtual Server.

4.3.7.1 Mapped IP

Internal private IP addresses are translated through NAT (Network Address Translation). If a server is located in the LAN network, it has a private IP address, and outside users cannot connect directly to LAN servers' private IP address. To connect to a LAN network server, outside users have to first connect to a real IP address of the WAN network, and the real IP is translated to a private IP of the LAN network. Mapped IP and Virtual Server are the two methods to translate the real IP into private IP. Mapped IP maps IP in one-to-one fashion; that means, all services of one real WAN IP address is mapped to one private LAN IP address.

Entering the Mapped IP window

Step 1. Click **Mapped IP** under the **Virtual Server** menu bar and the Mapped IP configuration window will appear.



Definition:

WAN IP: WAN IP Address.

Map to Virtual IP: The IP address which WAN maps to the virtual network in the server.

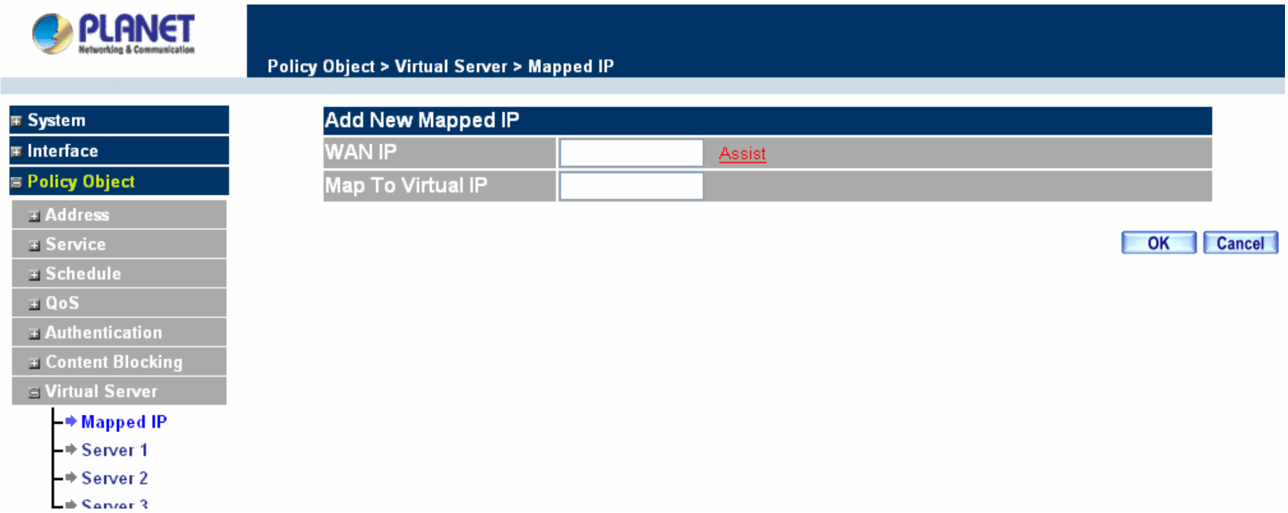
Configure: To change the setting, click Configure to modify the parameters; click delete to delete the setting.

Adding a new IP Mapping

Step 1. In the **Mapped IP** window, click the New Entry button. The Add New Mapped IP window will appear.

- **WAN IP**: select the WAN public IP address to be mapped.
- **Internal IP**: enter the LAN private IP address will be mapped 1-to-1 to the WAN IP address.

Step 2. Click **OK** to add new IP Mapping or click **Cancel** to cancel adding.



Policy Object > Virtual Server > Mapped IP

Add New Mapped IP	
WAN IP	Assist
Map To Virtual IP	

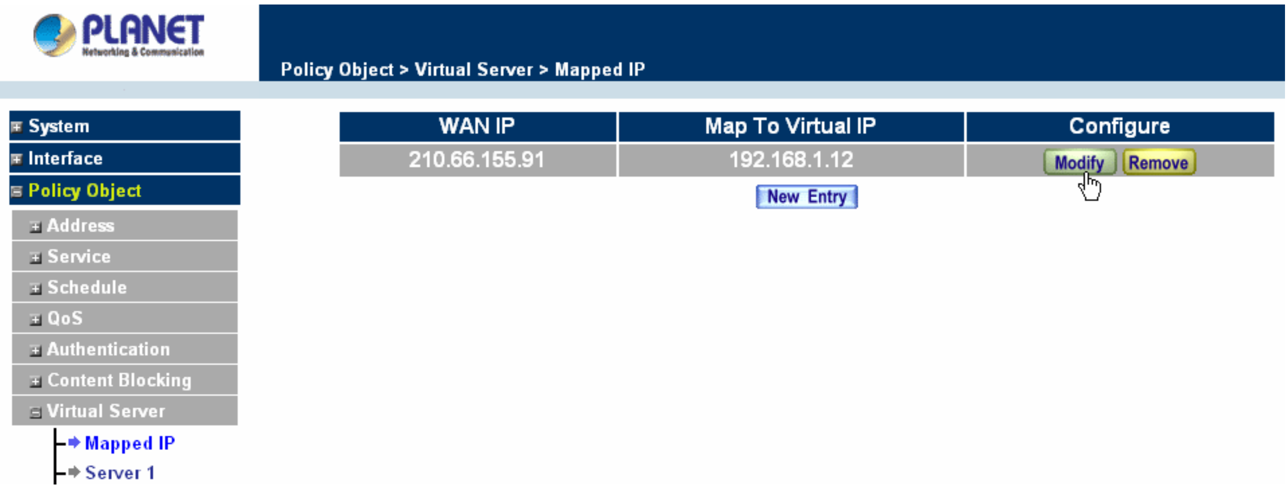
OK Cancel

Modifying a Mapped IP

Step 1. In the **Mapped IP** table, locate the Mapped IP you want it to be modified and click its corresponding Modify option in the Configure field.

Step 2. Enter settings in the Modify Mapped IP window.

Step 3. Click **OK** to save change or click **Cancel** to cancel.



Policy Object > Virtual Server > Mapped IP

WAN IP	Map To Virtual IP	Configure
210.66.155.91	192.168.1.12	Modify Remove

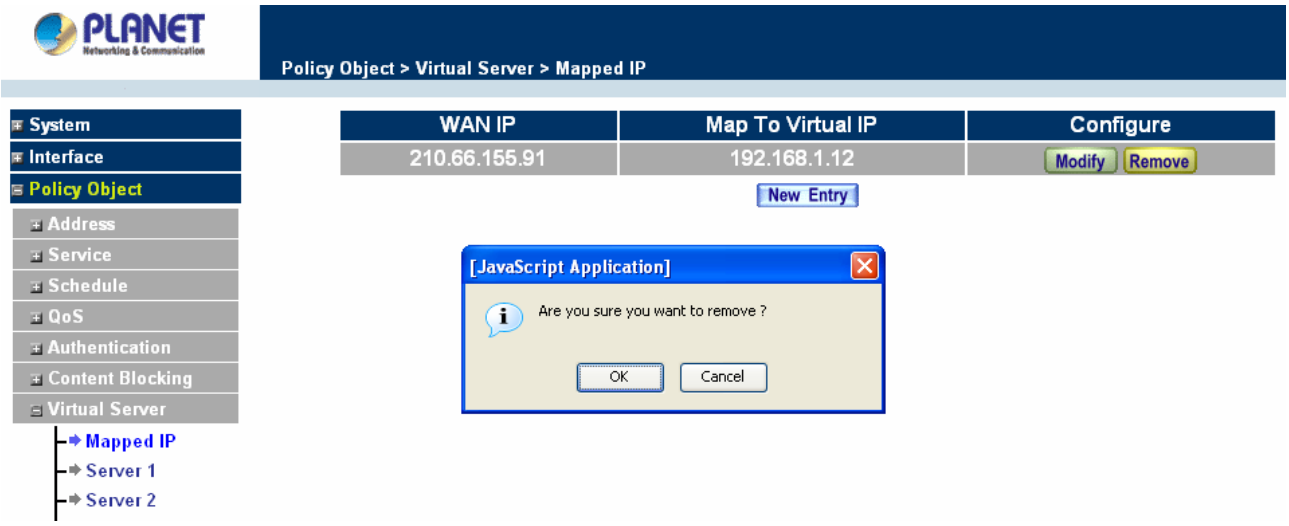
New Entry

NOTE: A Mapped IP cannot be modified if it has been assigned/used as a destination address of any Incoming policies.

Removing a Mapped IP

Step 1. In the Mapped IP table, locate the Mapped IP desired to be removed and click its corresponding Remove option in the Configure field.

Step 2. In the Remove confirmation pop-up window, click **OK** to remove the Mapped IP or click **Cancel** to cancel.


Policy Object > Virtual Server > Mapped IP

WAN IP	Map To Virtual IP	Configure
210.66.155.91	192.168.1.12	Modify Remove

New Entry

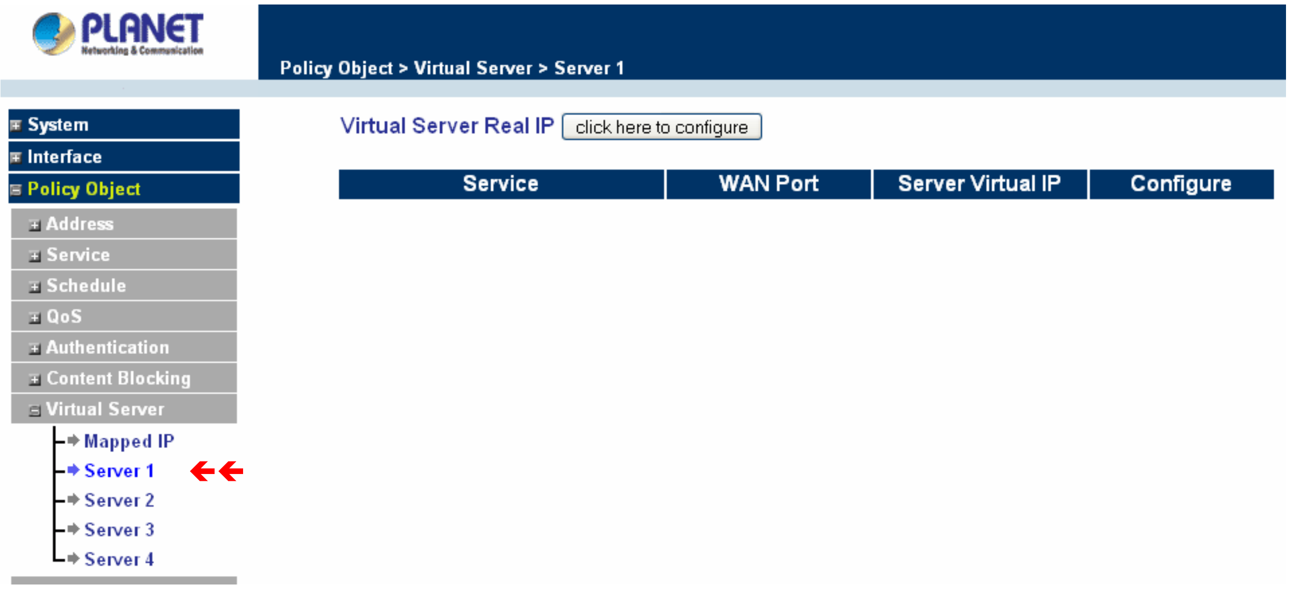
[JavaScript Application]

Are you sure you want to remove ?

OK Cancel

4.3.7.2 Virtual Server

Virtual server is a one-to-many mapping technique, which maps a real IP address from the WAN interface to private IP addresses of the LAN network. This function provides services or applications defined in the Service menu to enter into the LAN network. Unlike a mapped IP which binds a WAN IP to a LAN IP, virtual server binds WAN IP ports to LAN IP ports.


Policy Object > Virtual Server > Server 1

Virtual Server Real IP click here to configure

Service	WAN Port	Server Virtual IP	Configure

Definition:

Virtual Server Real IP: The WAN IP address configured by the virtual server. Click "**Click here to configure**" button to add a real IP address.

Service: The service names that provided by the virtual server.

WAN Port: The TCP/UDP ports that present the service items provided by the virtual server.

Server Virtual IP: The virtual IP which mapped by the virtual server.

Configure: To change the service configuration, click **Configure** to change the parameters; click **Delete** to delete the configuration.

This virtual server provides four real IP addresses, which means you can setup four virtual servers at most. The administrator can select Virtual Server1/2/3/4 under Virtual Server selection in the menu bar on the left hand side, click **Server Virtual IP** to add or change the virtual server IP address; click **"Click here to configure"** to add or change the virtual server service configuration.

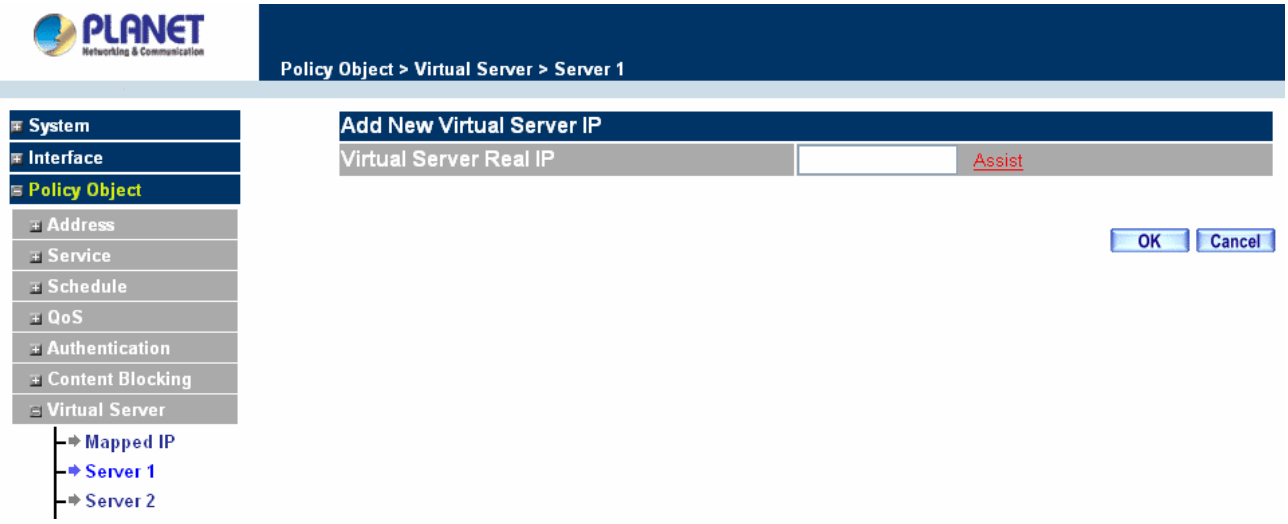
Configuring a Real IP for a Virtual Server

Step 1. Click an available virtual server from **Server 1/2/3/4** in the **Virtual Server** menu bar to enter the virtual server configuration window.

Step 2. Click the **click here to configure** button and the Add new Virtual Server IP window appears and asks for an IP address from the WAN network.

Step 3. Select an IP address from the drop-down list of available WAN network IP addresses.

Step 4. Click **OK** to add new Virtual Server or click **Cancel** to cancel adding.



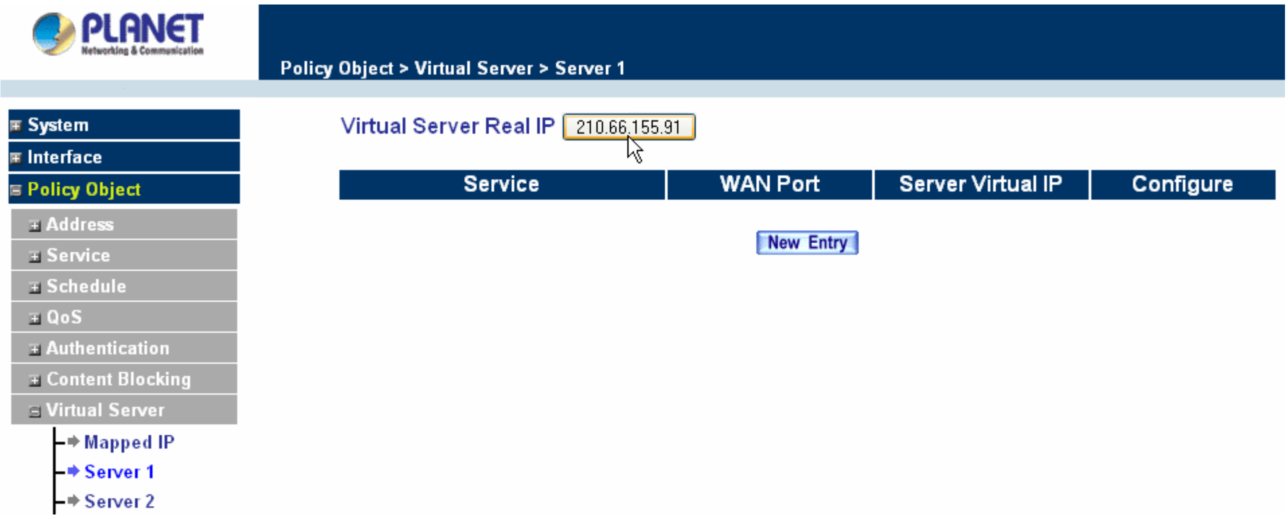
Modifying a Virtual Server IP Address

Step 1. Click the **Server 1/2/3/4** to modify the configuration under the **Virtual Server** menu bar. A new window appears displaying the IP address and service of the specified virtual server.

Step 2. Click on the Virtual Server's IP Address button at the top of the screen.

Step 3. Choose a new IP address from the drop-down list.

Step 4. Click **OK** to save new IP address or click **Cancel** to discard changes.



Policy Object > Virtual Server > Server 1

Virtual Server Real IP 210.66.155.91

Service	WAN Port	Server Virtual IP	Configure

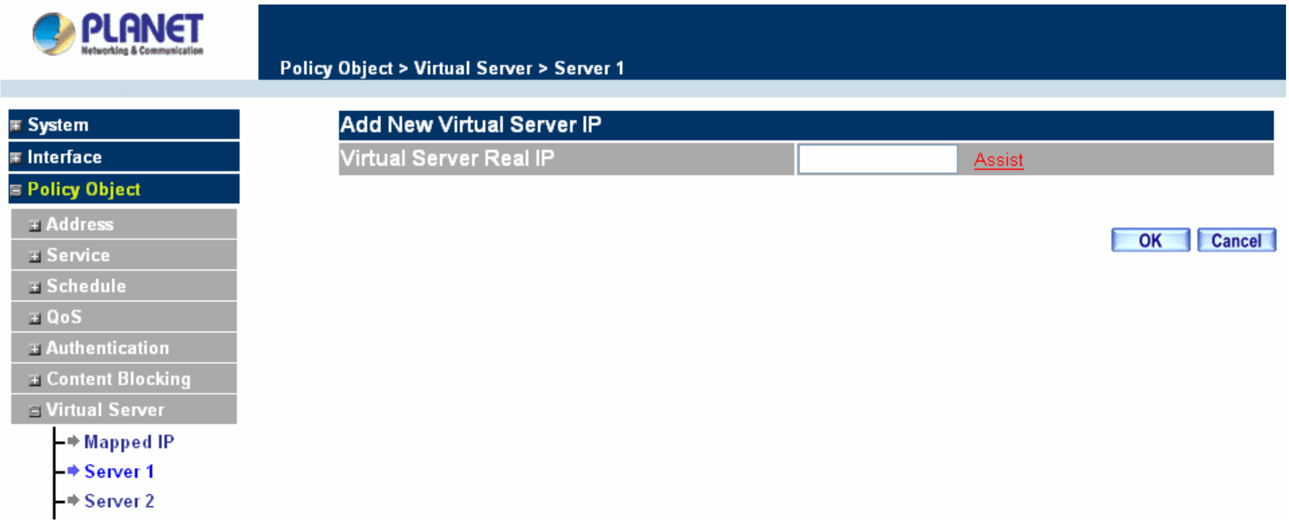
Removing a Virtual Server

Step 1. Click the virtual server to be removed in the corresponding Virtual Server option under the **Virtual Server** menu bar. A new window displaying the virtual server's IP address and service appears on the screen.

Step 2. Click the Virtual Server's IP Address button at the top of the screen.

Step 3. Delete the IP address.

Step 4. Click **OK** to remove the virtual server.



Policy Object > Virtual Server > Server 1

Add New Virtual Server IP

Virtual Server Real IP

Setting the Virtual Server's services

Step 1. For the Virtual Server which has already been set up with an IP address, click the New Service button in the table.

Step 2. In the Virtual Server Configurations window:

- **Virtual Server Real IP:** displays the WAN IP address assigned to the Virtual Server

- **Service (Port):** select the service from the pull down list that will be provided by the Real

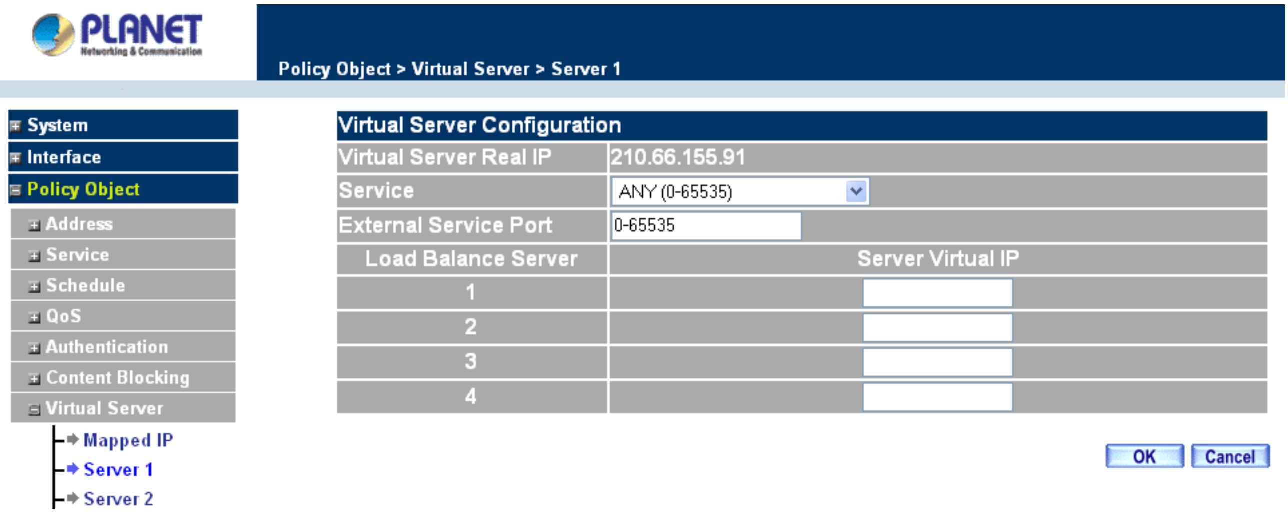
Server (Load Balance Server).

- **External Service Port:** Input the port number that the virtual server will use. Changing the Service will change the port number to match the service.
- **Load Balance Server:** The internal server IP address mapped by the virtual server. Four computer IP addresses can be set at most, and the load can be maintained in a balance by round robin algorithm.

Step 3. Enter the IP address of the LAN network server(s), to which the virtual server will be mapped. Up to four IP addresses can be assigned at most.

Step 4. Click **OK** to save the settings of the Virtual Server.

NOTE: The services in the drop-down list are all defined in the Pre-defined and Custom section of the **Service** menu.



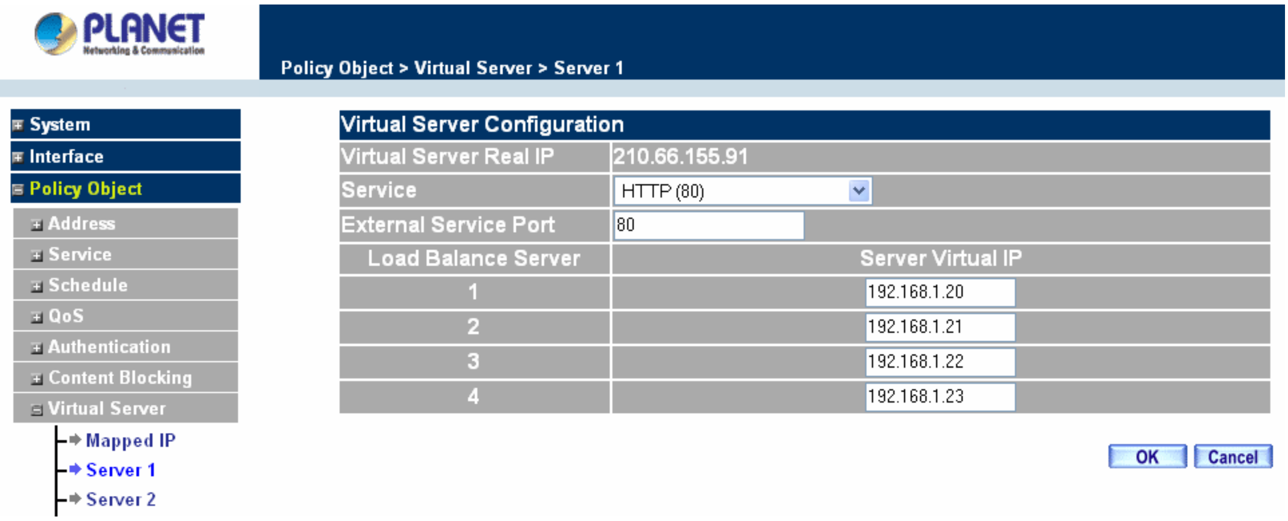
Virtual Server Configuration	
Virtual Server Real IP	210.66.155.91
Service	ANY (0-65535)
External Service Port	0-65535
Load Balance Server	Server Virtual IP
1	
2	
3	
4	

Adding New Virtual Server Service Configuration

Step 1. Select Virtual Server in the menu bar on the left hand side, and then select Server 1/2/3/4 sub-selections.

Step 2. In Server 1/2/3/4 Window, click "**New Entry**" button.

Step 3. Enter the parameters in the Virtual Server Configuration column.



Virtual Server Configuration	
Virtual Server Real IP	210.66.155.91
Service	HTTP (80)
External Service Port	80
Load Balance Server	Server Virtual IP
1	192.168.1.20
2	192.168.1.21
3	192.168.1.22
4	192.168.1.23

- **Virtual Server Real IP:** displays the WAN IP address assigned to the Virtual Server
- **Service (Port):** select the service from the pull down list that will be provided by the Real Server (Load Balance Server).
- **External Service Port:** Input the port number that the virtual server will use. Changing the Service will change the port number to match the service.
- **Load Balance Server:** The internal server IP address mapped by the virtual server. Four computer IP addresses can be set at most, and the load can be maintained in a balance by round robin algorithm.

Click **OK** to execute adding new virtual server service, or click **Cancel** to discard adding.

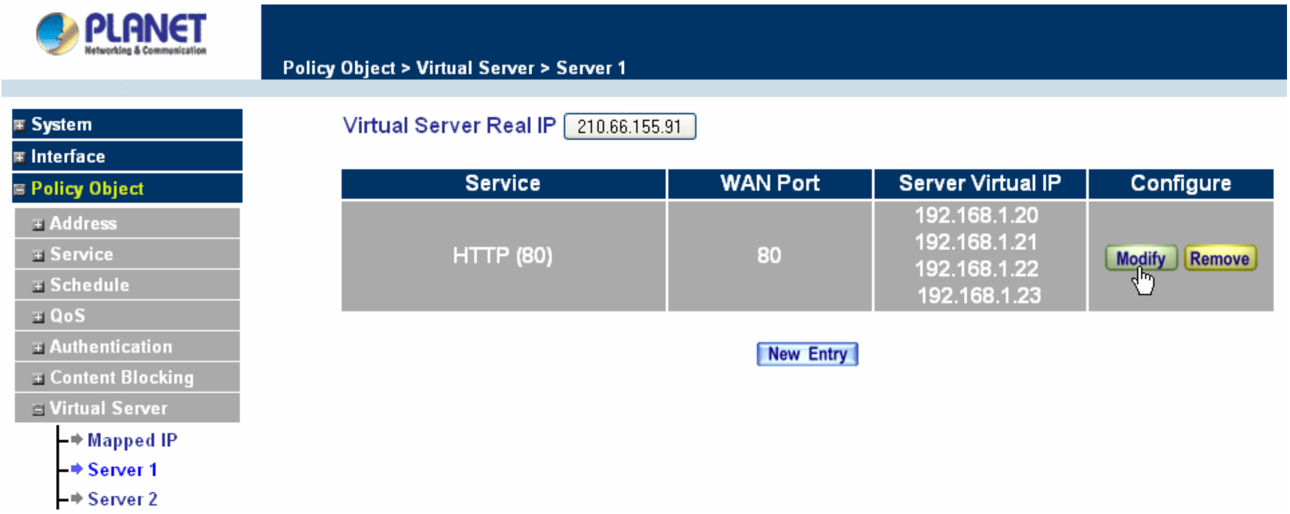
Remember to configure the service items of virtual server before you configure Policy, or the service names will not be shown in Policy.

Modifying the Virtual Server configurations

Step 1. In the Virtual Server window's service table, locate the name of the service desired to be modified and click its corresponding Modify option in the Configure field.

Step 2. In the Virtual Server Configuration window, enter the new settings.

Step 3. Click **OK** to save modifications or click **Cancel** to discard changes.



Policy Object > Virtual Server > Server 1

Virtual Server Real IP 210.66.155.91

Service	WAN Port	Server Virtual IP	Configure
HTTP (80)	80	192.168.1.20 192.168.1.21 192.168.1.22 192.168.1.23	Modify Remove

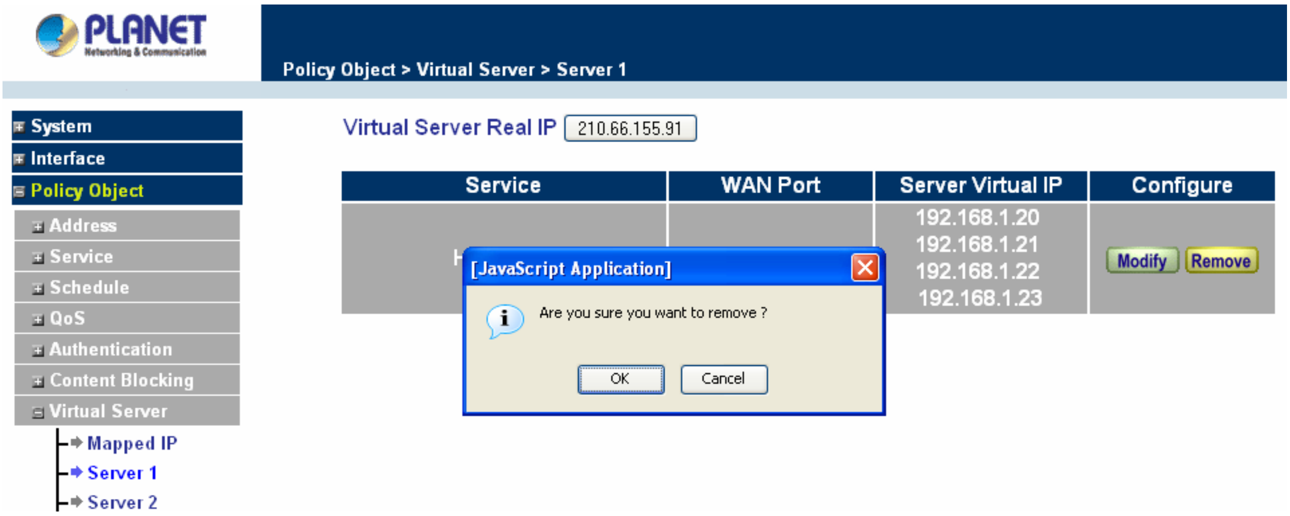
Click **OK** to execute the change of the virtual server, or click **Cancel** to discard changes.

NOTE: If the destination Network in Policy has set a virtual server, it will not be able to change or configure this virtual server, you have to remove this configuration of Policy, and then you can execute the modification or configuration.

Removing the Virtual Server service

Step 1. In the Virtual Server window's service table, locate the name of the service desired to be removed and click its corresponding Remove option in the Configure field.

Step 2. In the Remove confirmation pop-up box, click **OK** to remove the service or click **Cancel** to cancel removing.



Policy Object > Virtual Server > Server 1

Virtual Server Real IP 210.66.155.91

Service	WAN Port	Server Virtual IP	Configure
H		192.168.1.20 192.168.1.21 192.168.1.22 192.168.1.23	Modify Remove

[JavaScript Application]

Are you sure you want to remove ?

NOTE: If the destination Network in Policy has set a virtual server, it will not be able to change or configure this virtual server unless you have already removed this configuration of Policy.

4.3.8 VPN

The CS-500 adopts VPN to set up safe and private network service, and combine the remote Authentication system in order to integrate the remote network and PC of the enterprise. It also provides the remote users a safe encryption way to have best efficiency and encryption when delivering data. CS-500 provides two kinds of VPN service and the PPTP client.

IPSec Autokey: The system manager can create a VPN connection using Autokey IKE. Autokey IKE (Internet Key Exchange) provides a standard method to negotiate keys between two security gateways. It also can set up IPSec Lifetime and Preshared Key of the CS-500.

PPTP Server: The System Manager can set up VPN-PPTP Server functions at CS-500 in this chapter.

PPTP Client: The System Manager can set up VPN-PPTP Client functions at CS-500 in this chapter.

Tunnel: To define local and remote VPN device with related information, then the **Tunnel** entry can be selected in **Policy** in order to submit the further function to the VPN traffic.

What is New?

CS-500 isolates the **Tunnel** setting in order to allow **Policy** rule controlling VPN traffic. So user can filter the VPN packets with **QoS**, **IDP** rule, and record the connection in **Traffic Log** or **Statistic**. Hence, to set up a **Virtual Private Network** (VPN), you need to configure CS-500 with following setting:

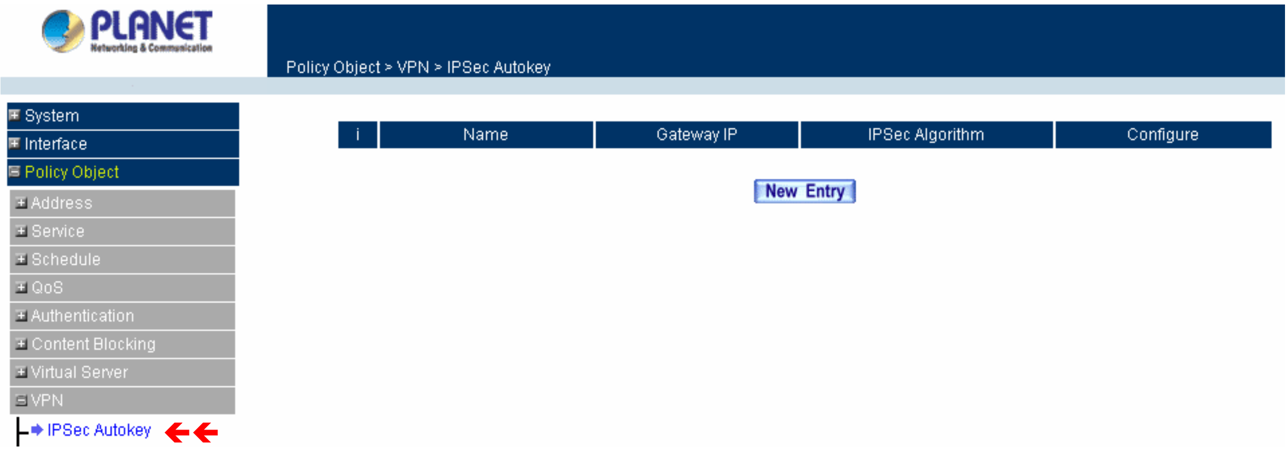
1. Configure **IPSec Autokey** for the encryption and authentication or **PPTP Server/Client** setting.
2. Configure **Tunnel** for the information of local and remote VPN device.
3. Configure **Incoming Policy** Rule to combine VPN traffic with QoS, IDP and the other function.

4.3.8.1 IPSec Autokey

This chapter describes steps to create a VPN connection using Autokey IKE. Autokey IKE (Internet Key Exchange) provides a standard method to negotiate keys between two security gateways. For example, with two Content Security Gateway devices, IKE allows new keys to be generated after a set amount of time has passed or a certain threshold of traffic has been exchanged.

Accessing the Autokey IKE window

Click **IPSec Autokey** under the VPN menu to enter the **IPSec Autokey** window. The **IPSec Autokey** table displays current configured VPNs.



i	Name	Gateway IP	IPSec Algorithm	Configure

The fields in the IPSec Autokey window are:

■ **Name:** The VPN name to identify the VPN tunnel definition. The name must be different for the two sites creating the tunnel.

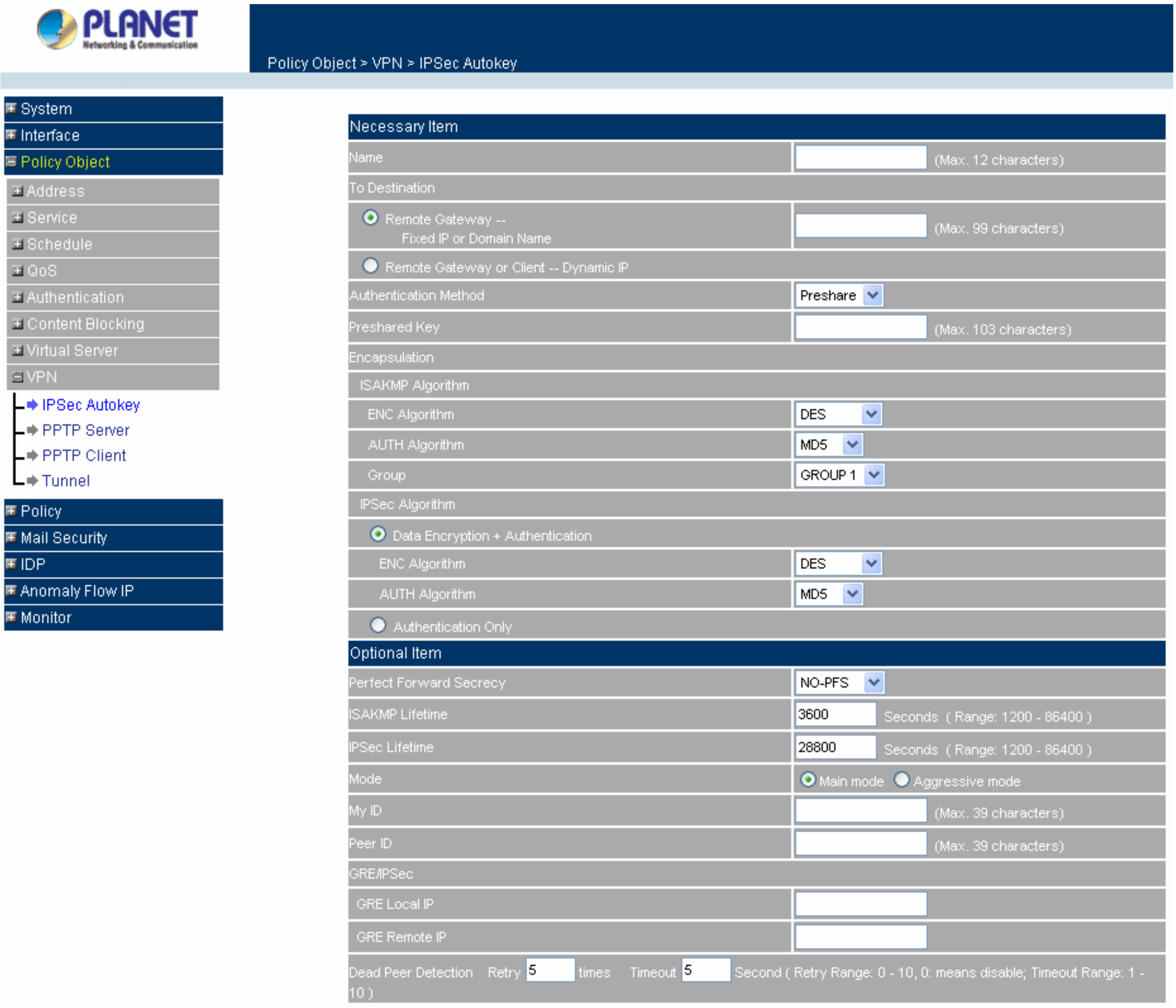
■ **Gateway IP:** The other side WAN interface IP address of VPN Gateway.

■ **IPSec Algorithm:** The display the Algorithm way.

■ **Configure:** Modify and Delete.

Adding the Autokey IKE

Step 1: Click the **New Entry** button and the **VPN Auto Keyed Tunnel** window will appear. It divides into two parts of the setting, **Necessary Item** and **Optional Item**.



Necessary Item	
Name	(Max. 12 characters)
To Destination	
● Remote Gateway -- Fixed IP or Domain Name	(Max. 99 characters)
○ Remote Gateway or Client -- Dynamic IP	
Authentication Method	Preshare
Preshared Key	(Max. 103 characters)
Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	DES
AUTH Algorithm	MD5
Group	GROUP 1
IPSec Algorithm	
● Data Encryption + Authentication	
ENC Algorithm	DES
AUTH Algorithm	MD5
○ Authentication Only	
Optional Item	
Perfect Forward Secrecy	NO-PFS
ISAKMP Lifetime	3600 Seconds (Range: 1200 - 86400)
IPSec Lifetime	28800 Seconds (Range: 1200 - 86400)
Mode	● Main mode ○ Aggressive mode
My ID	(Max. 39 characters)
Peer ID	(Max. 39 characters)
GRE/IPSec	
GRE Local IP	
GRE Remote IP	
Dead Peer Detection Retry 5 times Timeout 5 Second (Retry Range: 0 - 10, 0: means disable; Timeout Range: 1 - 10)	

Step 2: Configure **Necessary Item** paremeters.

Name: Specify a name for the VPN rule.

To Destination:

■ **Remote Gateway – Fixed IP or Domain Name:** Specify the fixed IP address or domain name of the remote side VPN gateway.

- **Remote Gateway or Client – Dynamic IP:** Select **Remote Gateway or Client** if there is only one user or device and dials up to Internet with PPPoE or cable modem.

Preshared Key: The IKE VPN must be defined with a Preshared Key. The Key may be up to 128 bytes long.

Encapsulation

ISAKMP Algorithm

- **ENC Algorithm:** ESP Encryption Algorithm. ESP (Encapsulating Security Payload) provides security for the payload (data) sent through the VPN tunnel. Generally, you will want to enable both Encryption and Authentication. The available encryption algorithms including: 56 bit DES-CBC, 168-bit 3DES-CBC, AES 128-bit, AES 192-bit or AES 256-bit encryption algorithm. The default algorithm 56 bit DES-CBC.
- **AUTH Method:** Authentication Method. Selects MD5 (128-bit hash) or SHA-1 (160-bit hash) authentication algorithm. In general, SHA-1 is more secured than MD5. The default algorithm is MD5.
- **Group:** Selects Group 1 (768-bit modulus), Group 2 (1024-bit modulus) or Group 5 (1536-bit modulus). The larger the modulus, the more secure the generated key is. However, the larger the modulus, the longer the key generation process takes. Both side of VPN tunnels must agree to use the same group. The default algorithm is Group 1.

IPSec Algorithm: Select Data Encryption + Authentication or Authentication Only.

Data Encryption + Authentication

- **Encryption Algorithm:** Selects 56 bit DES-CBC, 168-bit 3DES-CBC, AES 128-bit, AES 192-bit or AES 256-bit encryption algorithm. The default algorithm is 56 bit DES-CBC.
- **Authentication Algorithm:** Selects MD5 (128-bit hash) or SHA-1 (160-bit hash) authentication algorithm. In general, SHA-1 is more secured than MD5. The default algorithm is MD5.

Authentication Only: Select this function the IPSec Algorithm will only be anthenticated with preshared key.

Step 3: Configure **Optional Item** paremeters if necessary.

- **Perfect Forward Secrecy:** Select Group 1, Group 2 or Group 5 to enhances security by changing the IPsec key at regular intervals, and ensuring that each key has no relationship to the previous key. The default is NO-PFS.
- **ISAKMP Lifetime:** New keys will be generated whenever the lifetime of the old keys is exceeded. The Administrator may enable this feature if needed and enter the lifetime in seconds to re-key. The default is 3600 seconds (one hours). Selection of small values could lead to frequent re-keying, which could affect performance.
- **IPSec Lifetime:** New keys will be generated whenever the lifetime of the old keys is exceeded. The Administrator may enable this feature if needed and enter the lifetime in seconds to re-key. The default is 28800 seconds (eight hours). Selection of small values could lead to frequent re-keying, which could affect performance.
- **Mode:** Select Main mode or Aggressive mode algorithm.

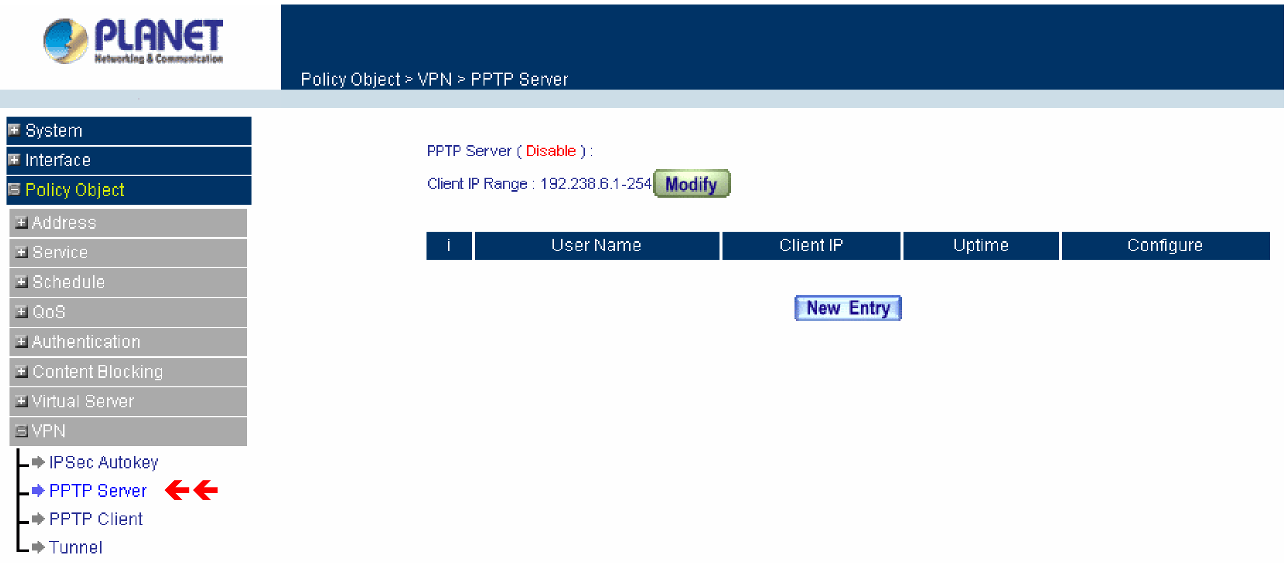
- **My ID/Peer ID:** My ID and Peer ID are optional parameters. If we choose to enter My ID/ Peer ID, they couldn't be the same. For instance, My ID is 11.11.11.11 and Peer ID is 22.22.22.22. If you want to use number or text, add @ in the front, for instance, @123A and @abcd123.
- **GRE/IPSec:** Select GRE/IPSec (Generic Routing Encapsulation) packet seal technology. You may enter IP to be identified for both VPN gateways.
- **Dead Peer Detection :** Configure the timing to detect the VPN status. If failed, CS-500 will disconnect the VPN tunnel.

For the complete VPN setting, you can refer to the example for more detail information.

4.3.8.2 PPTP Server

This function allows the remote client dialup to your local network and access local resources by PPTP (Point to Point Tunnel Protocol) client software.

Entering the PPTP Server window: Select **VPN→PPTP Server**.



PPTP Server (Disable) :

Client IP Range : 192.238.6.1-254

i	User Name	Client IP	Uptime	Configure

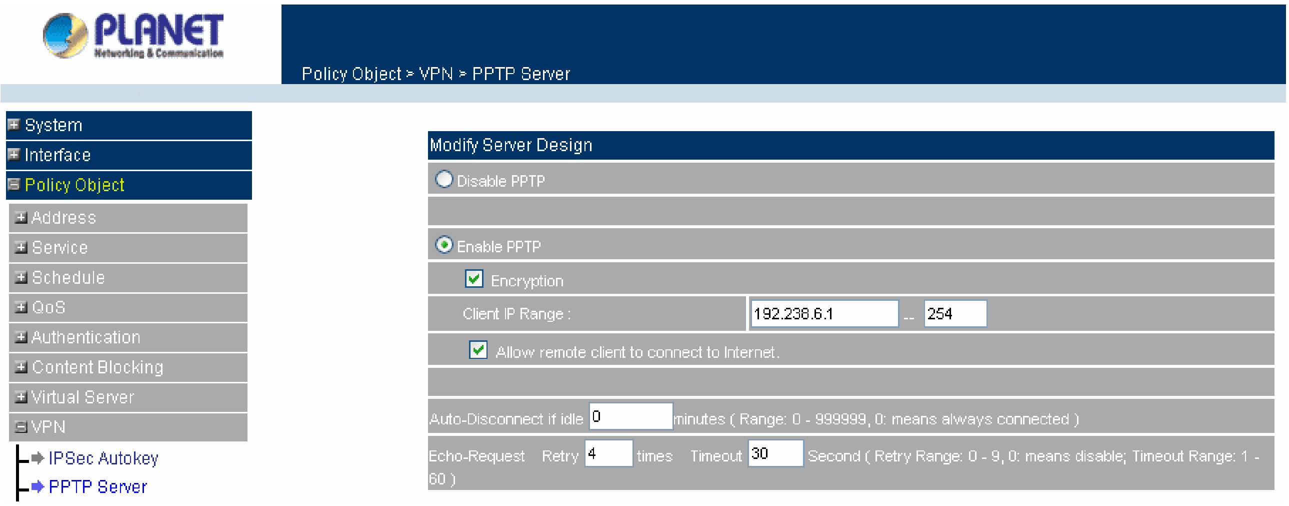
- **PPTP Server**：Click **Modify** to select Enable or Disable.
- **Client IP Range**: Display the IP addresses range for PPTP Client connection.
- **User Name**：Displays the PPTP Client user's name for authentication.
- **Client IP**：Displays the PPTP Client's IP address for authentication.
- **Uptime**：Displays the connection time between PPTP Server and Client.
- **Configure**：Click **Modify** to modify the PPTP Client settings or click **Remove** to remove the item.

Modifying PPTP Server Design

Step 1. Select **VPN→PPTP Server**.

Step 2. Click **Modify** after the Client IP Range.

Step 3. In the **Modify** Server Design Window, enter appropriate settings.



Modify Server Design

○ Disable PPTP

● Enable PPTP

☑ Encryption

Client IP Range : 192.238.6.1 _ 254

☑ Allow remote client to connect to Internet.

Auto-Disconnect if idle 0 minutes (Range: 0 - 999999, 0: means always connected)

Echo-Request Retry 4 times Timeout 30 Second (Retry Range: 0 - 9, 0: means disable; Timeout Range: 1 - 60)

- **Disable PPTP:** Check to disable PPTP Server.
- **Enable PPTP:** Check to enable PPTP Server.

  Encryption: the default is set to disabled.

  Client IP Range: Enter the IP range allocated for PPTP Clients when they connect to the PPTP server.
- **Allow remote client to connect to Internet:** Check to allow remote PPTP client accessing Internet via PPTP tunnel.
- **Auto-Disconnect if idle □ minutes:** Configure this device to disconnect to the PPTP Server when there is no activity for a predetermined period of time. To keep the line always connected, set the number to 0.
- **Echo-Request:** Configure the timing to detect the VPN status. If failed, CS-500 will disconnect the VPN tunnel.

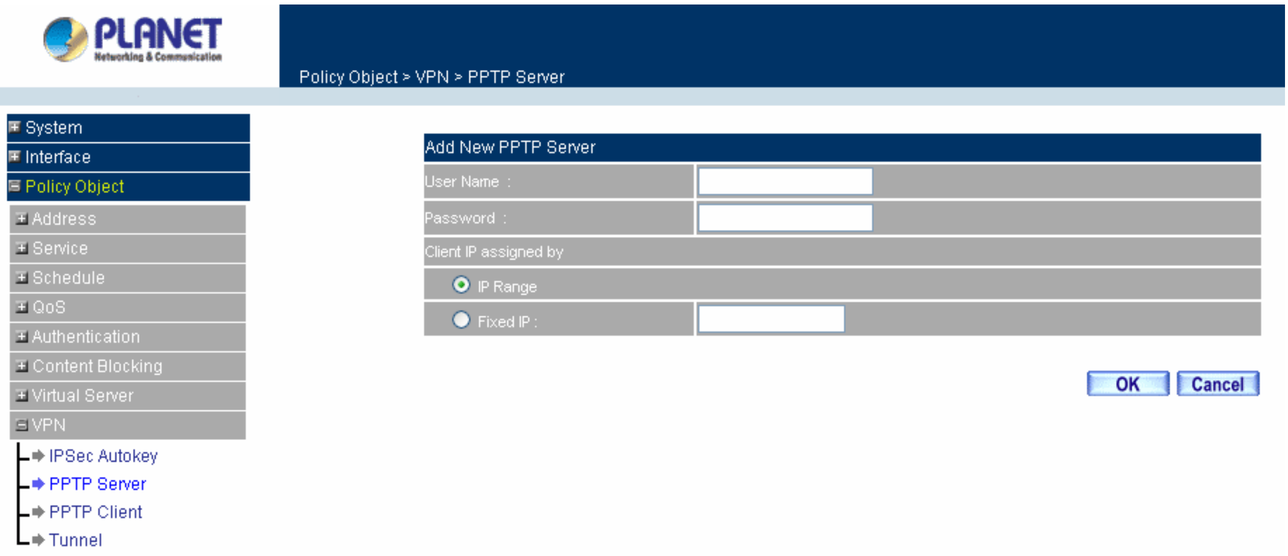
Step 4. Click **OK** to save modifications or click **Cancel** to cancel modifications

Adding PPTP Server

Step 1. Select **VPN→PPTP Server**. Click **New Entry.**

Step 2. Enter appropriate settings in the following window.

- User name: Specify the PPTP client. This should be unique.
- Password: Specify the PPTP client password.
- Client IP assigned by:
  1. IP Range: check to enable auto-allocating IP for PPTP client to connect.
  2. Fixed IP: check and enter a fixed IP for PPTP client to connect.



Add New PPTP Server	
User Name :	
Password :	
Client IP assigned by	
● IP Range	
○ Fixed IP :	

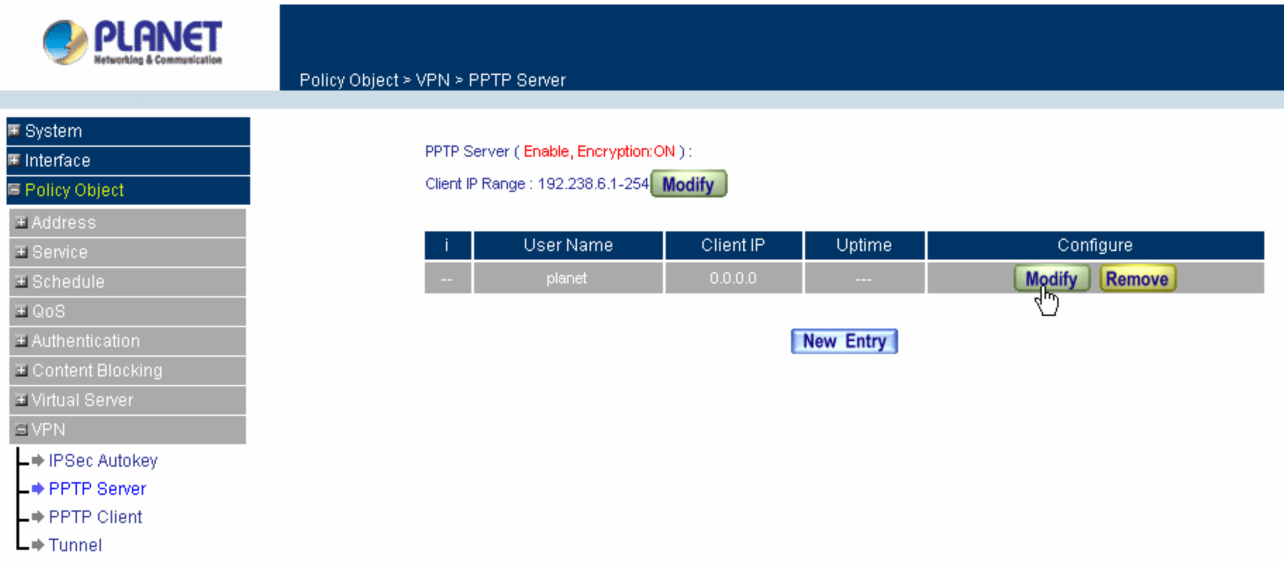
Step 3. Click **OK** to save modifications or click **Cancel** to cancel modifications.

Modifying PPTP Server

Step 1. Select **VPN→PPTP Server**.

Step 2. In the **PPTP Server** window, find the PPTP server that you want to modify. Click **Configure** and click **Modify**.

Step 3. Enter appropriate settings.



PPTP Server (Enable, Encryption:ON) :

Client IP Range : 192.238.6.1-254

i	User Name	Client IP	Uptime	Configure
--	planet	0.0.0.0	---	Modify Remove

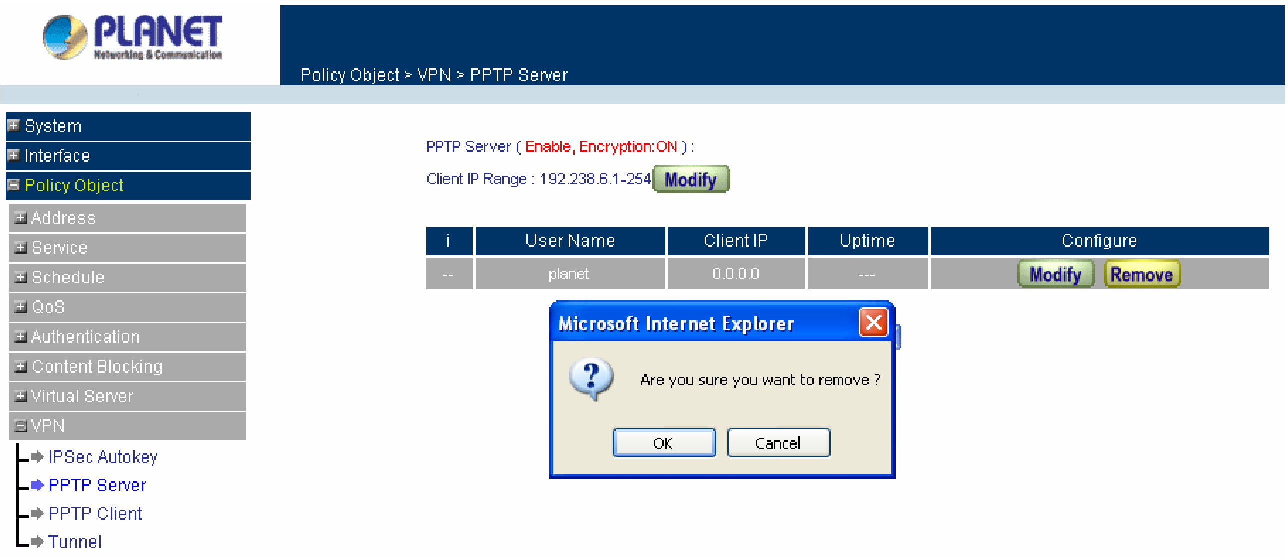
Step 4. Click **OK** to save modifications or click **Cancel** to cancel modifications

Removing PPTP Server

Step 1. Select **VPN→PPTP Server**.

Step 2. In the **PPTP Server** window, find the PPTP server that you WAN t to modify. Click **Configure** and click **Remove**.

Step 3. Click **OK** to remove the PPTP server or click **Cancel** to exit without removing.



Policy Object > VPN > PPTP Server

PPTP Server (Enable, Encryption:ON) :

Client IP Range : 192.238.6.1-254 Modify

i	User Name	Client IP	Uptime	Configure
--	planet	0.0.0.0	---	Modify Remove

Microsoft Internet Explorer

Are you sure you want to remove ?

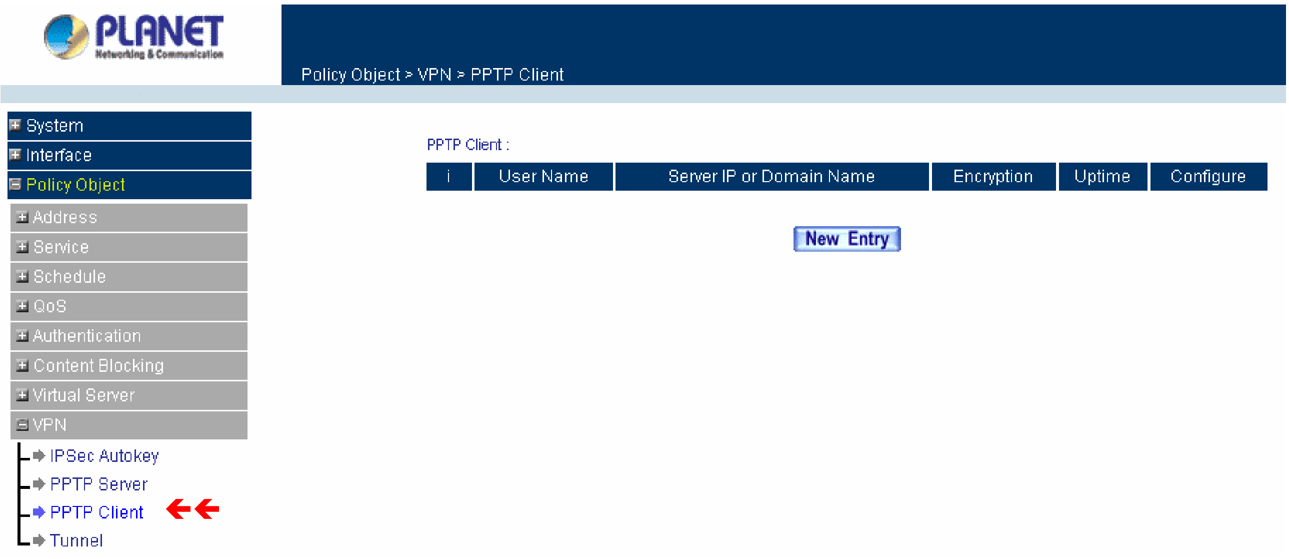
OK Cancel

4.3.8.3 PPTP Client

This function allows the Content Security Gateway dial-up to remote PPTP server and accesses the network resources on remote network.

Entering the PPTP Client window

Step 1. Select **VPN→PPTP Client**.



Policy Object > VPN > PPTP Client

PPTP Client :

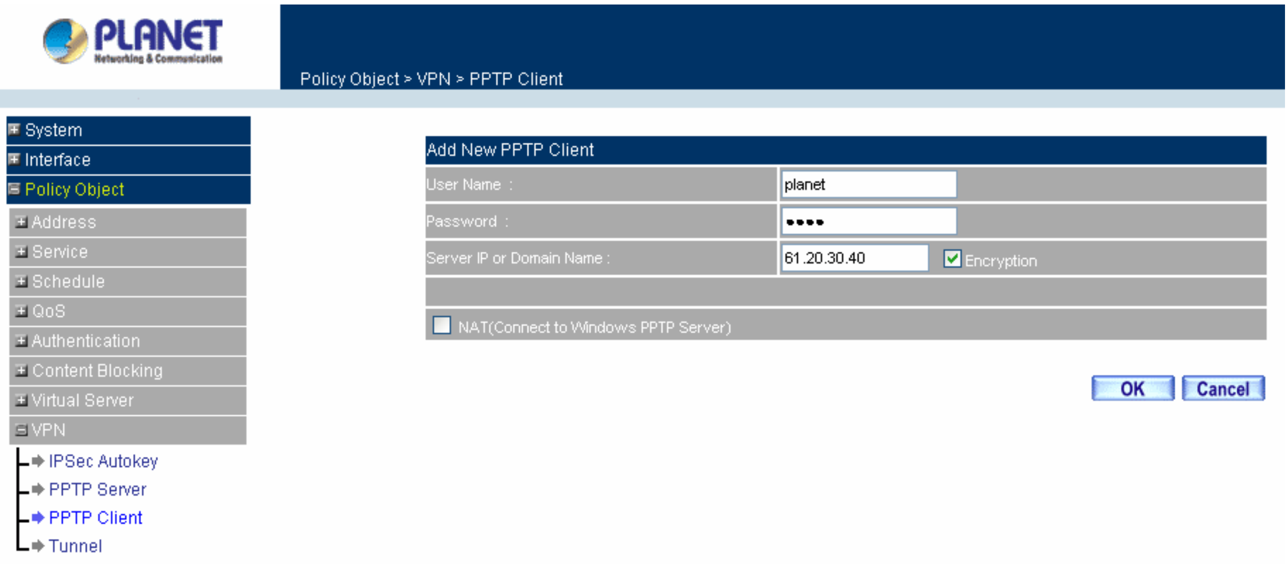
i	User Name	Server IP or Domain Name	Encryption	Uptime	Configure

New Entry

- **User Name**：Displays the PPTP Client user's name for authentication.
- **Server IP or Domain Name**：Displays the PPTP Server's IP address or Domain name.
- **Encryption**：Displays the PPTP Client Encryption ON or OFF.
- **Uptime**：Displays the connection time between PPTP Server and Client.
- **Configure**：Click **Modify** to modify the PPTP Client settings or click **Remove** to remove the item.

Adding a PPTP Client

Step 1. Select **VPN→PPTP Client**.



Add New PPTP Client

User Name :	planet
Password :	••••
Server IP or Domain Name :	61.20.30.40 ☑ Encryption
☐ NAT(Connect to Windows PPTP Server)	

Step 2. Configure the parameters.

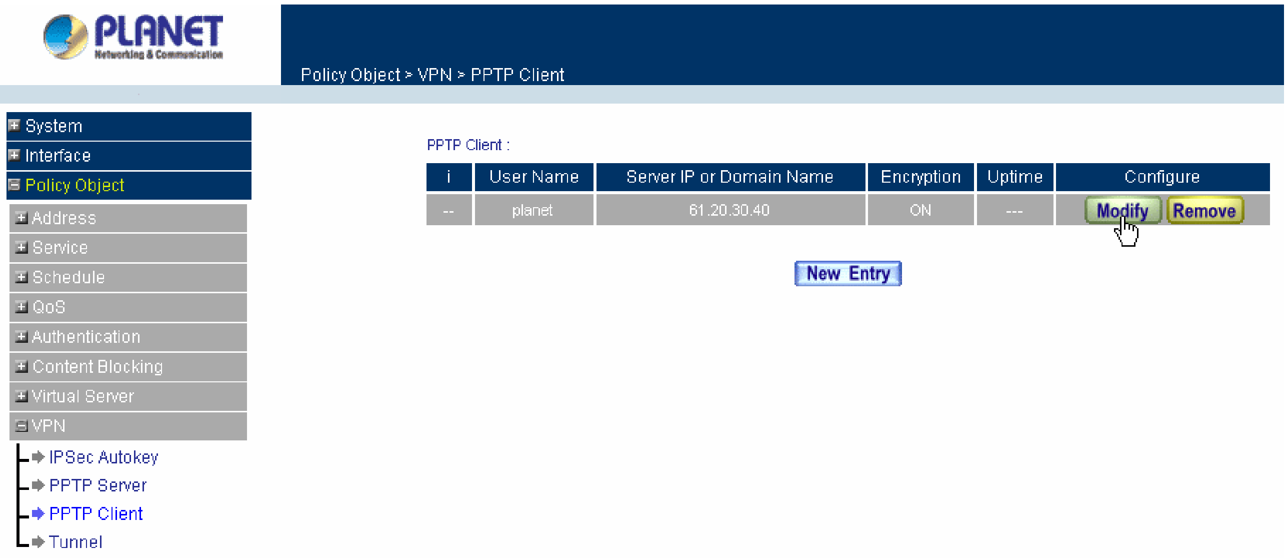
- **User name:** Specify the PPTP client. This should be unique.
- **Password:** Specify the PPTP client password.
- **Server IP or Domain Name:** Enter the PPTP Server's IP address.
- **Encryption:** Enable or Disabled the Encryption.
- **NAT (Connect to Windows PPTP Server):** Select this function to setup the connection with PPTP VPN Client of CS-500 and Windows PPTP Server.

Modifying PPTP Client

Step 1. Select **VPN→PPTP Client**.

Step 2. In the **PPTP Client** window, find the PPTP server that you want to modify and click **Modify**.

Step 3. Enter appropriate settings.



PPTP Client :

i	User Name	Server IP or Domain Name	Encryption	Uptime	Configure
--	planet	61.20.30.40	ON	---	Modify Remove

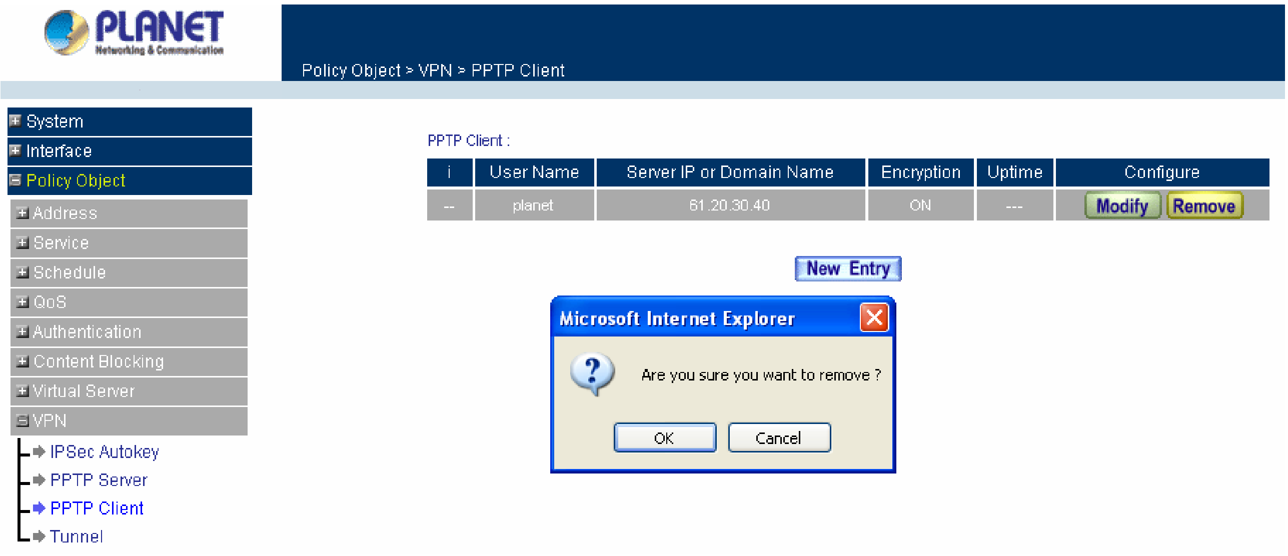
Step 4. Click **OK** to save modifications or click **Cancel** to cancel modifications

Removing PPTP Client

Step 1. Select **VPN→PPTP Client**.

Step 2. In the **PPTP Client** window, find the PPTP client that you want to modify and click **Remove**.

Step 3. Click **OK** to remove the PPTP client or click **Cancel** to exit without removal.



PPTP Client :

i	User Name	Server IP or Domain Name	Encryption	Uptime	Configure
--	planet	61.20.30.40	ON	---	Modify Remove

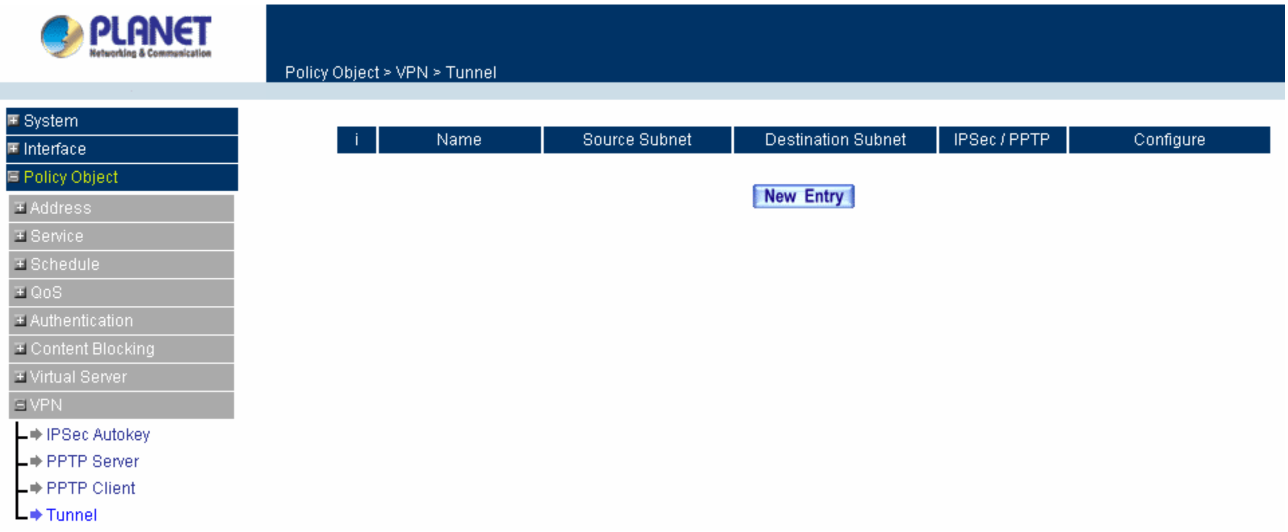
Are you sure you want to remove ?

4.3.8.4 Tunnel

This function allows to be configured the related information for local and remote VPN device, then to select the **Tunnel** entry in **Policy** rule for combining the further function.

Entering the Tunnel window

Step 1. Select **VPN→Tunnel**.



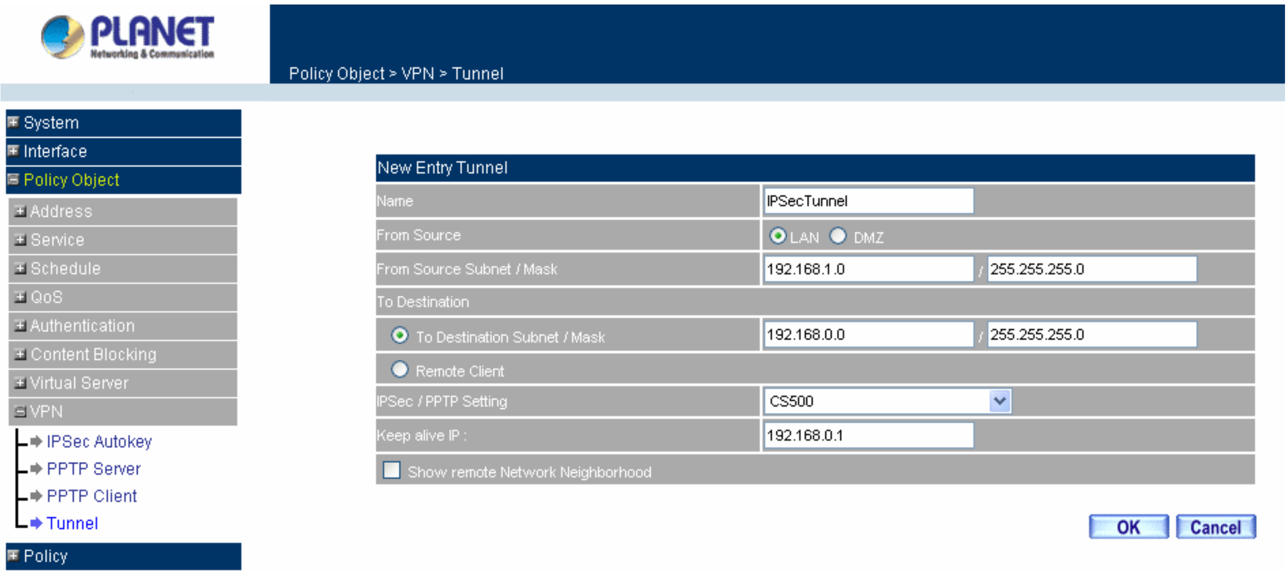
i	Name	Source Subnet	Destination Subnet	IPSec / PPTP	Configure

Step 2. Configure the parameters

- **Name:** Specify the Tunnel name. This should be unique and can not be the same as the name of IPSec Autokey rule.
- **Source Subnet:** Specify the source LAN network subnet.
- **Destination Subnet:** Specify the destination LAN network subnet.
- **IPSec/PPTP:** Indicate the Tunnel type for IPSec or PPTP.
- **Configure**：Click **Modify** to modify the PPTP Client settings, **Pause** to stop the VPN tunnel, or **Remove** to remove the item.

Adding a Tunnel

Step 1. Select **VPN→Tunnel**.



New Entry Tunnel

Name	IPSecTunnel
From Source	● LAN ○ DMZ
From Source Subnet / Mask	192.168.1.0 / 255.255.255.0
To Destination	
● To Destination Subnet / Mask	192.168.0.0 / 255.255.255.0
○ Remote Client	
IPSec / PPTP Setting	CS500
Keep alive IP :	192.168.0.1
□ Show remote Network Neighborhood	

Step 2. Configure the parameters

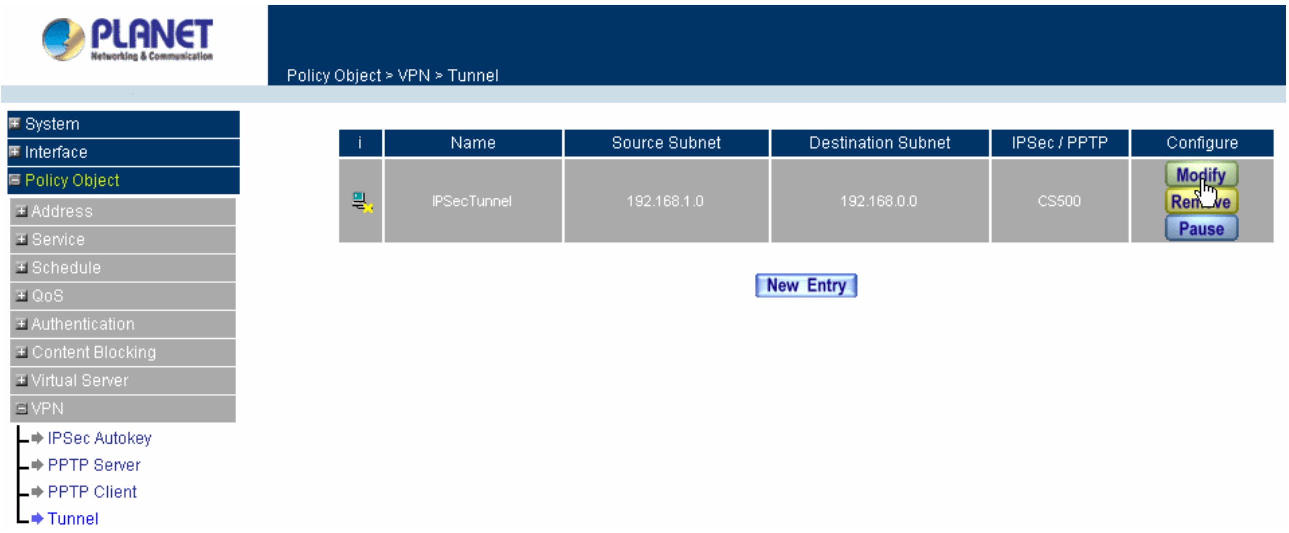
- **Name:** Specify the Tunnel name. This should be unique and can not be the same as the name of IPSec Autokey rule.
- **From Source:** Specify the VPN source to LAN or DMZ site.
- **From Source Subnet / Mask:** Specify the source LAN network subnet and Mask.
- **To Destination:**
  - **To Destination Subnet / Mask:** Specify the destination LAN network subnet and Mask.
  - **Remote Client:** Select **Remote Client** if there is only one user and dials up to Internet with PPPoE or cable modem.
- **IPSec/PPTP Setting:** Select the specific VPN tunnel for this Tunnel rule, you need to pre-define IPSec or PPTP setting first.
- **Keep Alive IP:** Specify **Remote Gateway**'s LAN IP address to keep alive the VPN tunnel
- **Show remote Network Neighborhood:** Select the remote Network Neighborhood enable to show.

Modifying a Tunnel

Step 1. Select **VPN→Tunnel**.

Step 2. In the **Tunnel** window, find the Tunnel that you want to modify and click **Modify**.

Step 3. Enter appropriate settings.

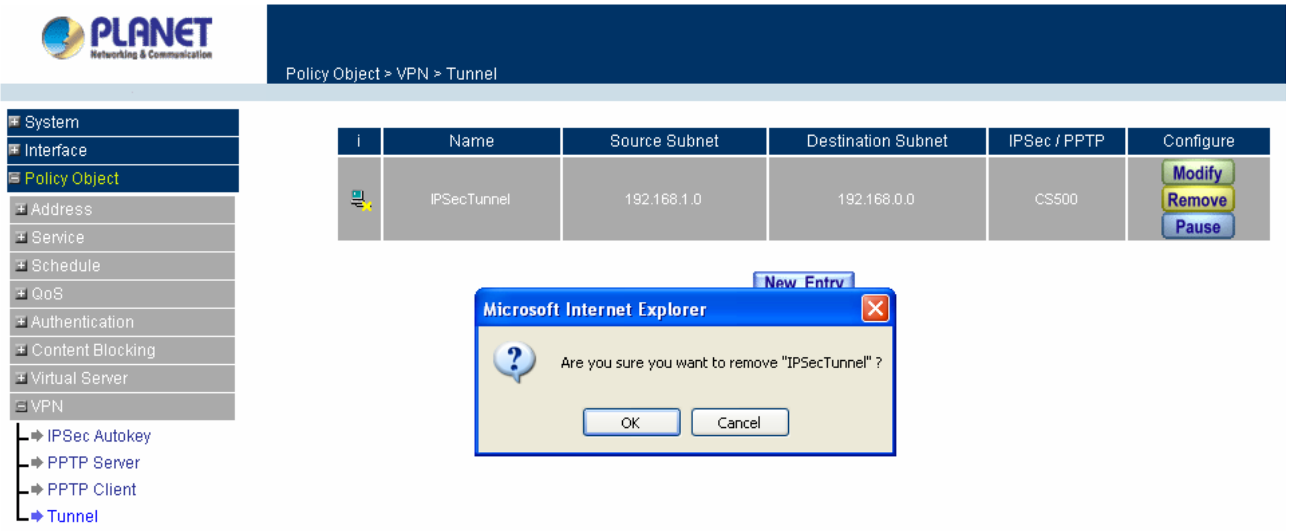


i	Name	Source Subnet	Destination Subnet	IPSec / PPTP	Configure
	IPSecTunnel	192.168.1.0	192.168.0.0	CS500	Modify Remove Pause

Removing Tunnel

Step 1. Select **VPN→Tunnel**.

Step 2. In the **Tunnel** window, find the Tunnel that you want to modify and click **Remove**.



i	Name	Source Subnet	Destination Subnet	IPSec / PPTP	Configure
	IPSecTunnel	192.168.1.0	192.168.0.0	CS500	Modify Remove Pause

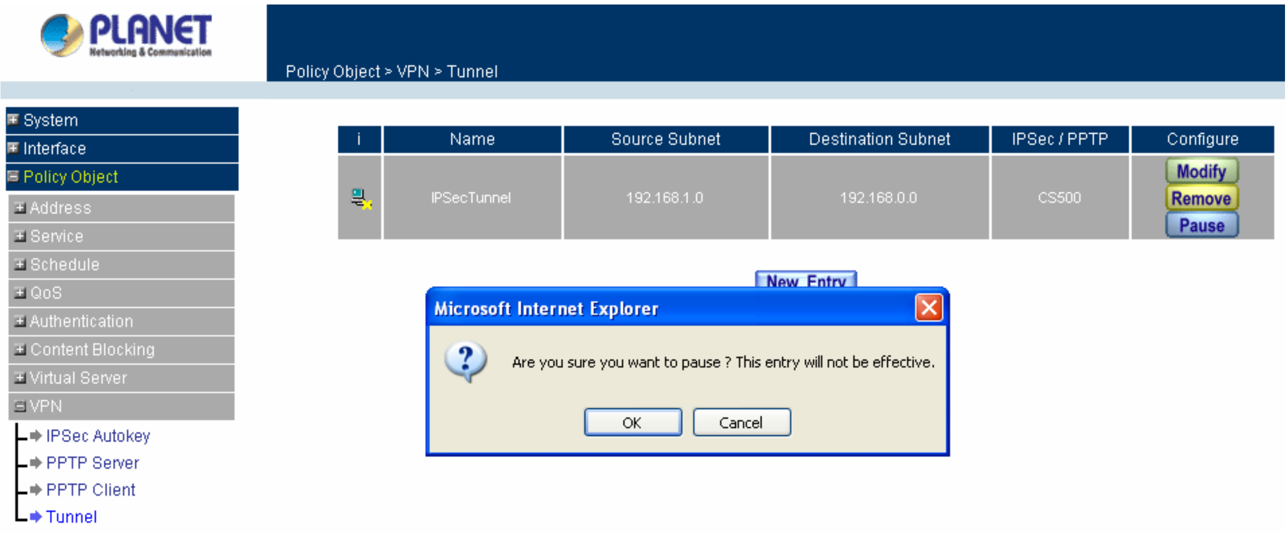
Are you sure you want to remove "IPSecTunnel" ?

Click **OK** to remove the PPTP client or click **Cancel** to exit without removal.

Pausing a Tunnel

Step 1. Select **VPN→Tunnel**.

Step 2. In the **Tunnel** window, find the Tunnel that you want to modify and click **Pause**.



i	Name	Source Subnet	Destination Subnet	IPSec / PPTP	Configure
	IPSecTunnel	192.168.1.0	192.168.0.0	CS500	Modify Remove Pause

Microsoft Internet Explorer

Are you sure you want to pause ? This entry will not be effective.

Step 3. When

There are 5 examples of VPN setting.

Example 1. Create a VPN connection between two Content Security Gateways.

Example 2. Create a VPN connection between the Content Security Gateway and Windows XP Professional VPN Client.

Example 3. Create a VPN connection between two Content Security Gateways using Aggressive mode Algorithm (3DES and MD5), and data encryption for IPSec Algorithm (3DES and MD5)

Example 4. Create a VPN connection between Content Security Gateway and PLANET VRT-311 VPN Router.

Example 1. Create a VPN connection between two Content Security Gateways.

Preparation Task:

Company A External IP is 61.11.11.11
Internal IP is 192.168.10.X

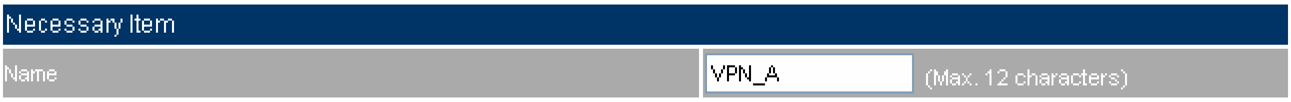
Company B External IP is 211.22.22.22
Internal IP is 192.168.20.X

To Allow Company A, 192.168.10.100 create a VPN connection with company B, 192.168.20.100 for downloading the sharing file.

The Gateway of Company A is 192.168.10.1. The settings of company A are as the following.

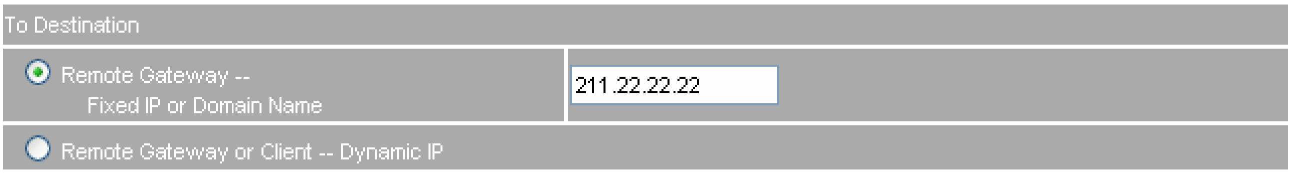
Step 1. Enter the default IP of Company A's Content Security Gateway, 192.168.10.1. Click VPN in the menu bar on the left hand side, and then select the sub-select IPSec Autokey. Click Add.

Step 2. Enter the VPN name, VPN_A in IPSec Autokey window.



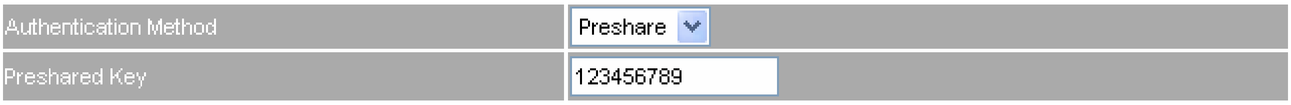
Necessary Item	
Name	VPN_A (Max. 12 characters)

Step 3. In To Destination table, choose Remote Gateway-Fixed IP or Domain Name, enter the IP address desired to be connected.



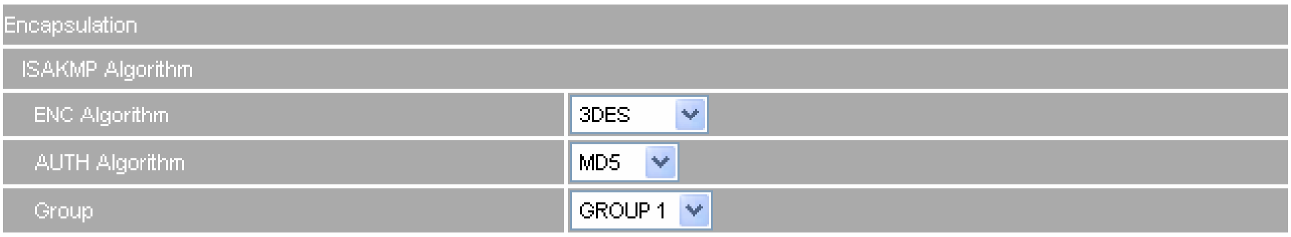
To Destination	
● Remote Gateway -- Fixed IP or Domain Name	211.22.22.22
○ Remote Gateway or Client -- Dynamic IP	

Step 4. In Authentication Method Table enters the Preshared Key.



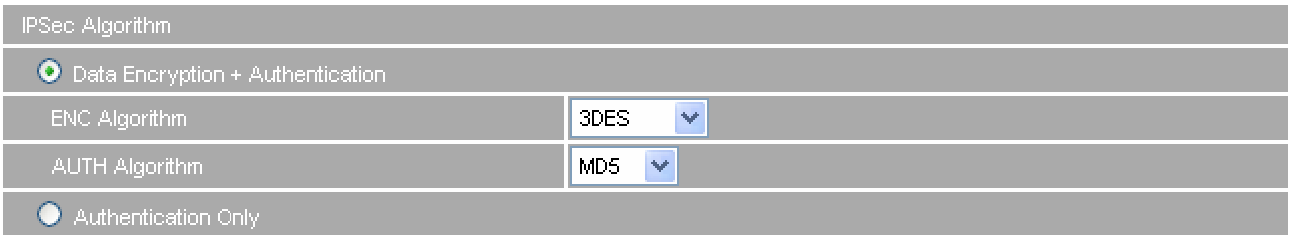
Authentication Method	Preshare
Preshared Key	123456789

Step 5. In Encapsulation or Authentication table, choose ISAKMP Algorithm. For communication via VPN, we choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm. And select Group 1 to connect.



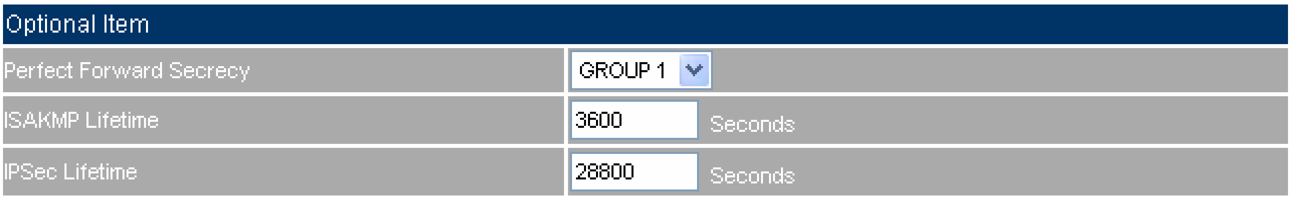
Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	3DES
AUTH Algorithm	MD5
Group	GROUP 1

Step 6. In IPSec Algorithm Table, choose Data Encryption + Authentication. We choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm.



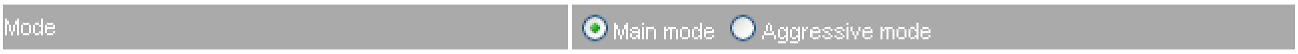
IPSec Algorithm	
● Data Encryption + Authentication	
ENC Algorithm	3DES
AUTH Algorithm	MD5
○ Authentication Only	

Step 7. Choose GROUP 1 as the Perfect Forward Secrecy setting, and leave the default setting with 28800 seconds in IPSec Lifetime and 3600 seconds for ISAKMP Lifetime.



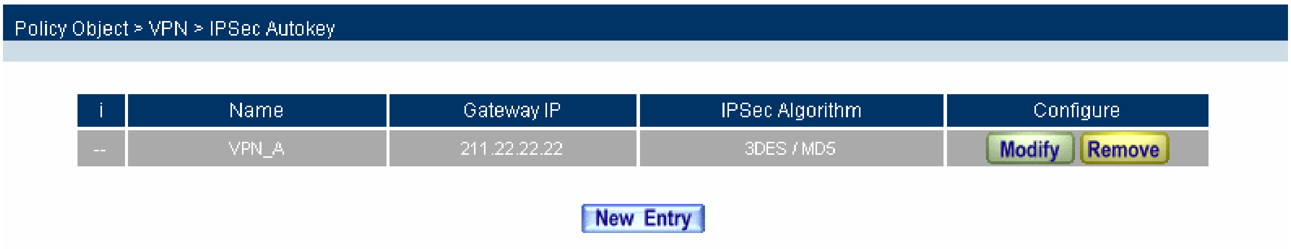
Optional Item	
Perfect Forward Secrecy	GROUP 1
ISAKMP Lifetime	3600 Seconds
IPSec Lifetime	28800 Seconds

Step 8. Select main mode as the algorithm.



Mode	● Main mode ○ Aggressive mode

Step 9. Click OK to finish the IPSec Aotukey setting of Company A.



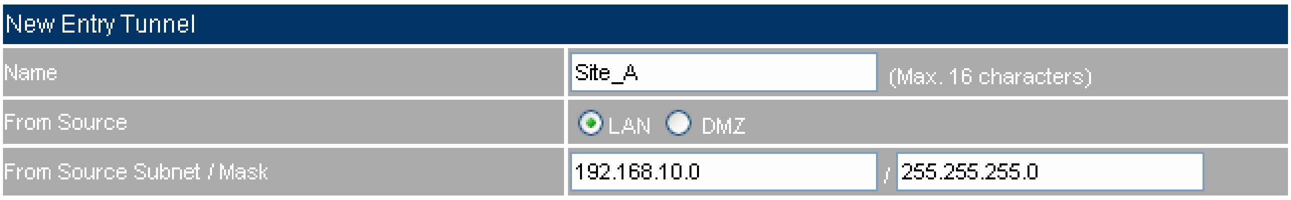
Policy Object > VPN > IPSec Autokey

i	Name	Gateway IP	IPSec Algorithm	Configure
--	VPN_A	211.22.22.22	3DES / MD5	Modify Remove

New Entry

Step 10. Click Tunnel and press New Entry to configure the further setting.

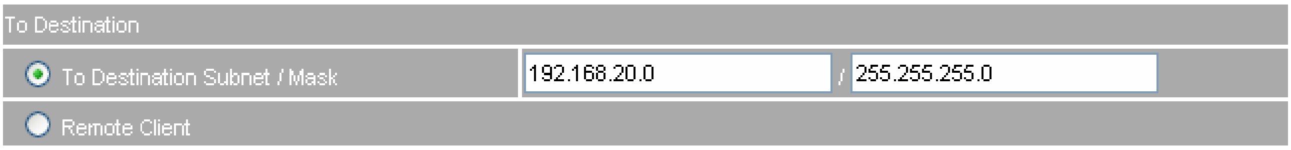
Step 11. Enter Site_A as the new tunnel name, and select LAN interface as the VPN source. Fill LAN IP subnet 192.168.10.0 with subnet mask IP 255.255.255.0.



New Entry Tunnel

Name	Site_A (Max. 16 characters)
From Source	● LAN ○ DMZ
From Source Subnet / Mask	192.168.10.0 / 255.255.255.0

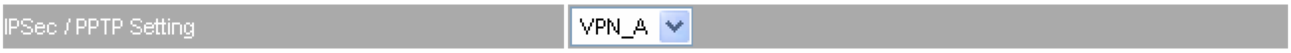
Step 12. In To Destination table, fill company B's subnet IP and mask, 192.168.20.0 and 255.255.255.0 respectively.



To Destination

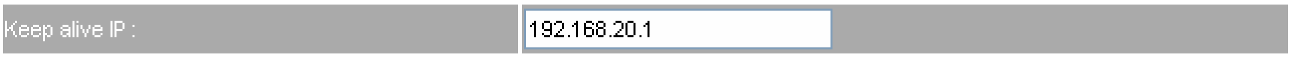
● To Destination Subnet / Mask	192.168.20.0 / 255.255.255.0
○ Remote Client	

Step 13. In IPSec / PPTP Setting, select VPN_A as the available tunnel.



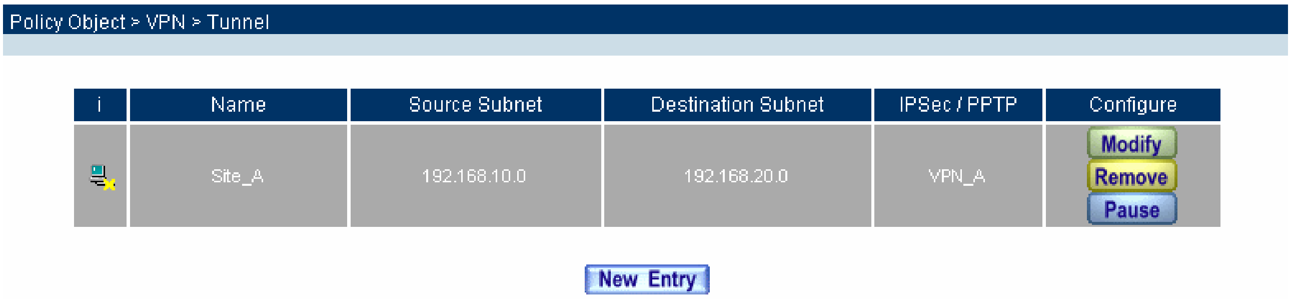
IPSec / PPTP Setting	VPN_A

Step 14. Fill company B's gateway IP 192.168.20.1 in Keep alive IP to keep VPN tunnel connecting.



Keep alive IP :	192.168.20.1

Step 15. Click OK to finish the Tunnel setting of Company A.

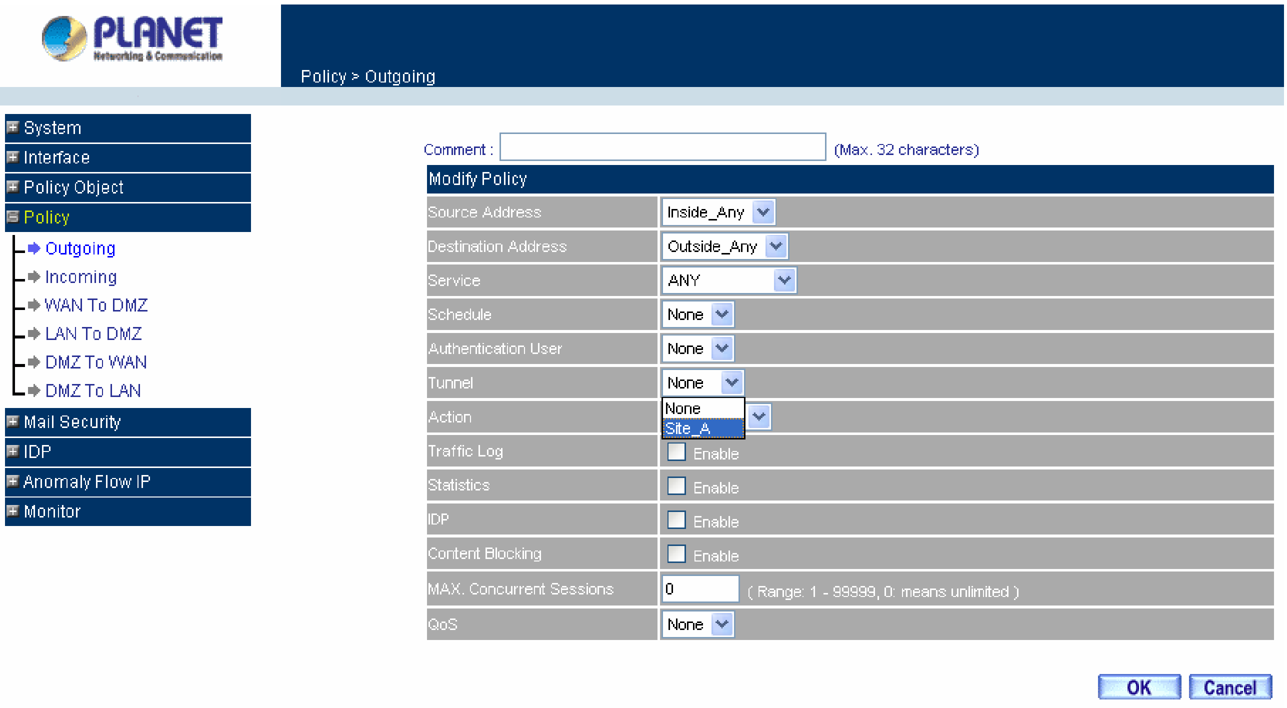


Policy Object > VPN > Tunnel

i	Name	Source Subnet	Destination Subnet	IPSec / PPTP	Configure
	Site_A	192.168.10.0	192.168.20.0	VPN_A	Modify Remove Pause

New Entry

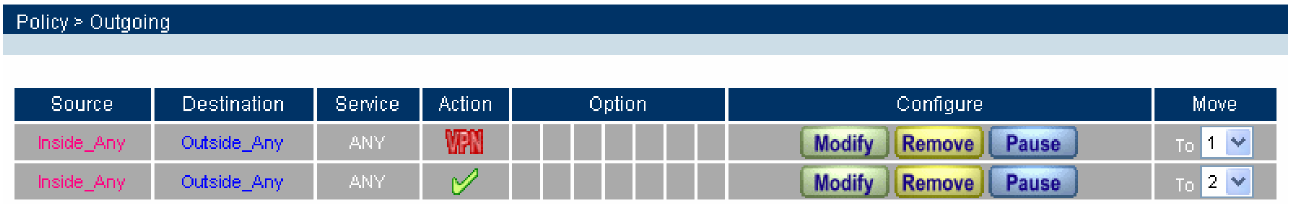
Step 16. If you want to configure bi-direction VPN connection, you should enable Tunnel setting in Outgoing and Incoming Policy.



Comment : (Max. 32 characters)

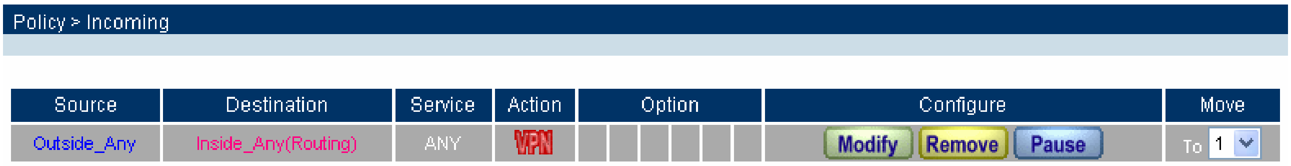
Modify Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
Tunnel	None None Site_A
Action	
Traffic Log	□ Enable
Statistics	□ Enable
IDP	□ Enable
Content Blocking	□ Enable
MAX. Concurrent Sessions	0 (Range: 1 - 99999, 0: means unlimited)
QoS	None

Outgoing Policy:


Policy > Outgoing

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	VPN		Modify Remove Pause	To 1
Inside_Any	Outside_Any	ANY	✓		Modify Remove Pause	To 2

Incoming Policy:

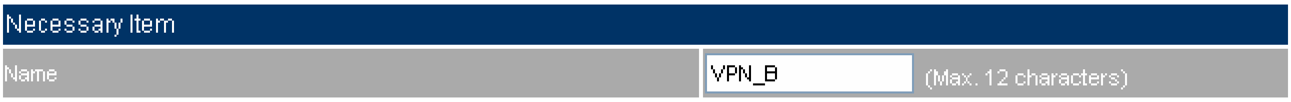

Policy > Incoming

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Inside_Any(Routing)	ANY	VPN		Modify Remove Pause	To 1

The Gateway of Company B is 192.168.20.1. The settings of company B are as the following.

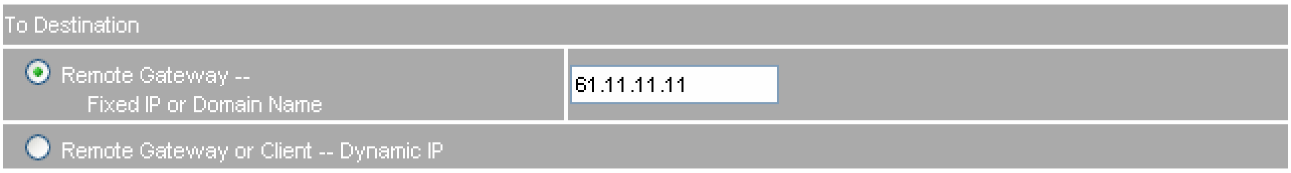
Step 1. Enter the default IP of Company B's Content Security Gateway, 192.168.20.1. Click VPN in the menu bar on the left hand side, and then select the sub-select IPSec Autokey. Click Add.

Step 2. Enter the VPN name, VPN_B in IPSec Autokey window.



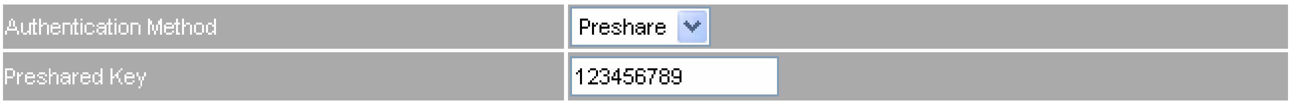
Necessary Item	
Name	VPN_B (Max. 12 characters)

Step 3. In To Destination table, choose Remote Gateway-Fixed IP or Domain Name, enter the IP address desired to be connected.



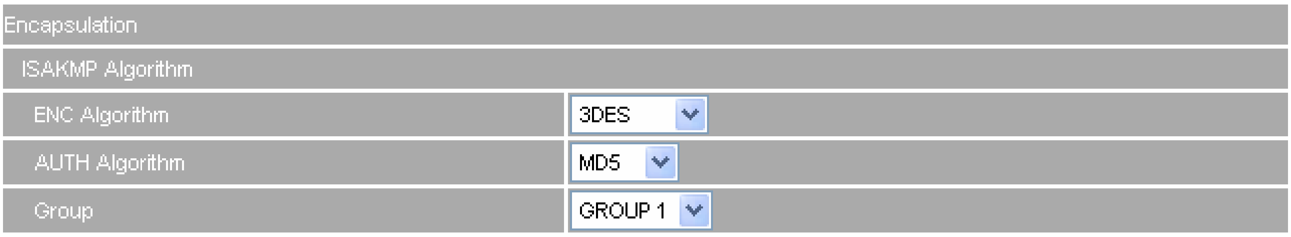
To Destination	
● Remote Gateway -- Fixed IP or Domain Name	61.11.11.11
○ Remote Gateway or Client -- Dynamic IP	

Step 4. In Authentication Method Table enters the Preshared Key.



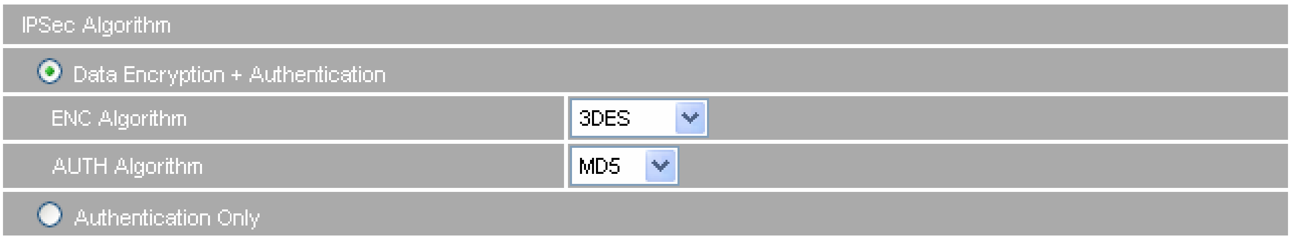
Authentication Method	Preshare
Preshared Key	123456789

Step 5. In Encapsulation or Authentication table, choose ISAKMP Algorithm. For communication via VPN, we choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm. And select Group 1 to connect.



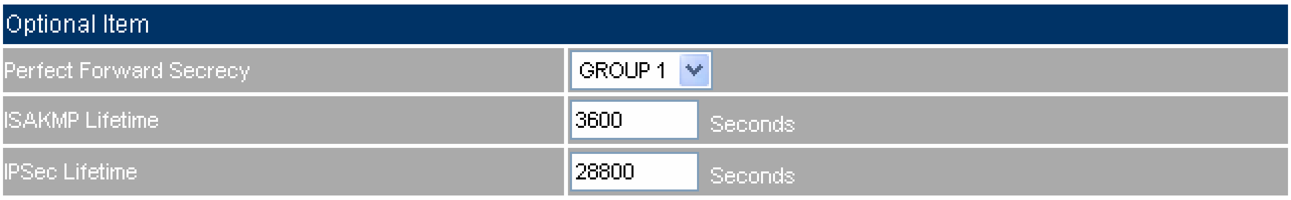
Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	3DES
AUTH Algorithm	MD5
Group	GROUP 1

Step 6. In IPSec Algorithm Table, choose Data Encryption + Authentication. We choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm.



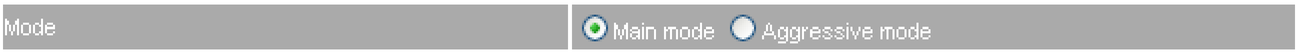
IPSec Algorithm	
● Data Encryption + Authentication	
ENC Algorithm	3DES
AUTH Algorithm	MD5
○ Authentication Only	

Step 7. Choose GROUP 1 as the Perfect Forward Secrecy setting, and leave the default setting with 28800 seconds in IPSec Lifetime and 3600 seconds for ISAKMP Lifetime.



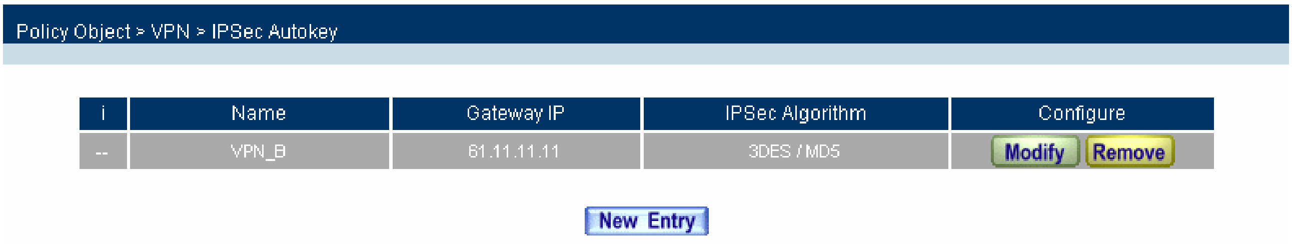
Optional Item	
Perfect Forward Secrecy	GROUP 1
ISAKMP Lifetime	3600 Seconds
IPSec Lifetime	28800 Seconds

Step 8. Select main mode as the algorithm.



Mode	● Main mode ○ Aggressive mode

Step 9. Click OK to finish the IPSec Aotukey setting of Company B.

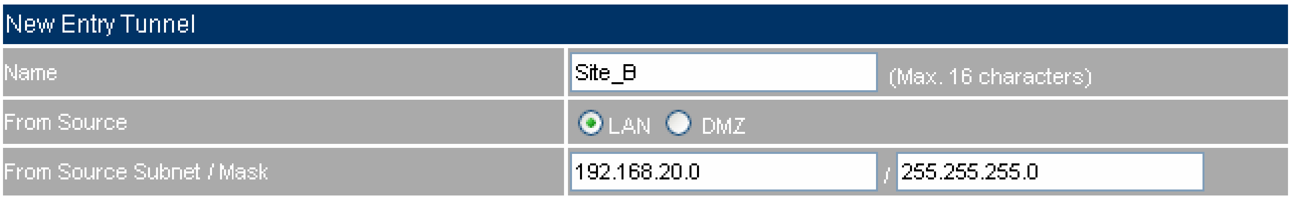


Policy Object > VPN > IPSec Autokey

i	Name	Gateway IP	IPSec Algorithm	Configure
--	VPN_B	61.11.11.11	3DES / MD5	Modify Remove

Step 10. Click Tunnel and press New Entry to configure the further setting.

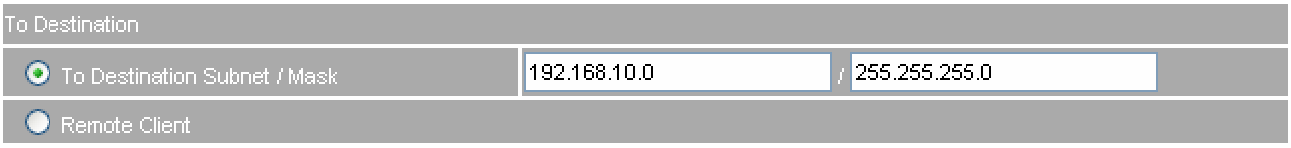
Step 11. Enter Site_B as the new tunnel name, and select LAN interface as the VPN source. Fill LAN IP subnet 192.168.20.0 with subnet mask IP 255.255.255.0.



New Entry Tunnel

Name	Site_B (Max. 16 characters)
From Source	● LAN ○ DMZ
From Source Subnet / Mask	192.168.20.0 / 255.255.255.0

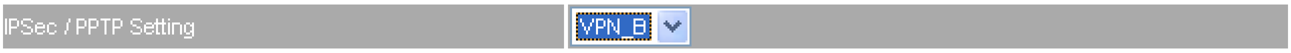
Step 12. In To Destination table, fill company B's subnet IP and mask, 192.168.10.0 and 255.255.255.0 respectively.



To Destination

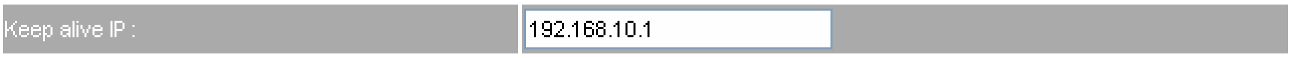
● To Destination Subnet / Mask	192.168.10.0 / 255.255.255.0
○ Remote Client	

Step 13. In IPSec / PPTP Setting, select VPN_B as the available tunnel.



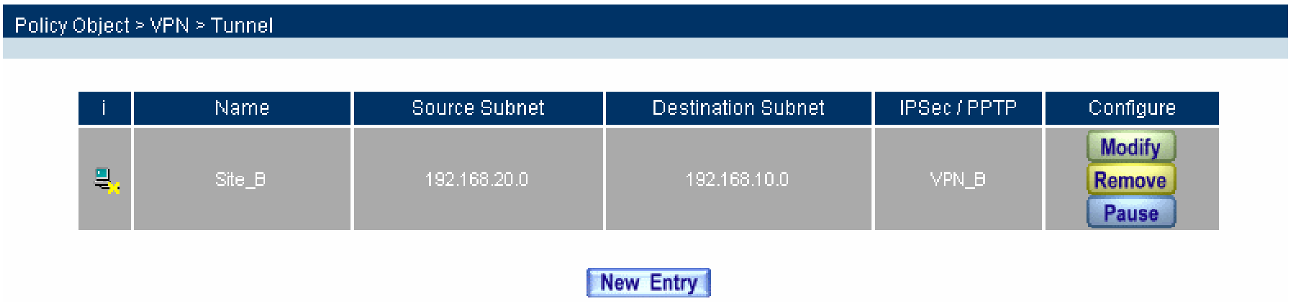
IPSec / PPTP Setting	VPN_B

Step 14. Fill company A's gateway IP 192.168.10.1 in Keep alive IP to keep VPN tunnel connecting.



Keep alive IP :	192.168.10.1

Step 15. Click OK to finish the Tunnel setting of Company B.



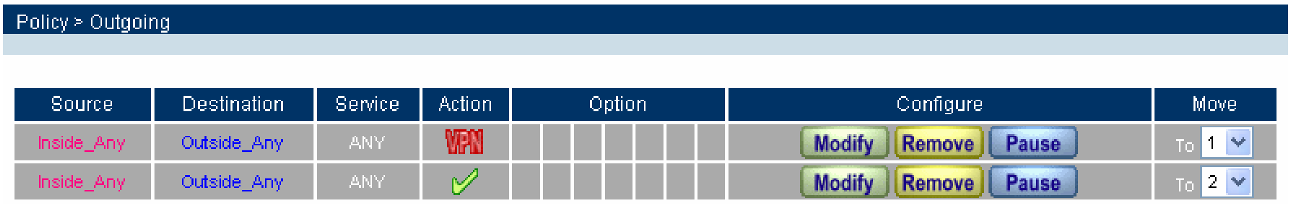
Policy Object > VPN > Tunnel

i	Name	Source Subnet	Destination Subnet	IPSec / PPTP	Configure
	Site_B	192.168.20.0	192.168.10.0	VPN_B	Modify Remove Pause

Step 16. If you want to configure bi-direction VPN connection, you should enable Tunnel setting in Outgoing

and Incoming Policy.

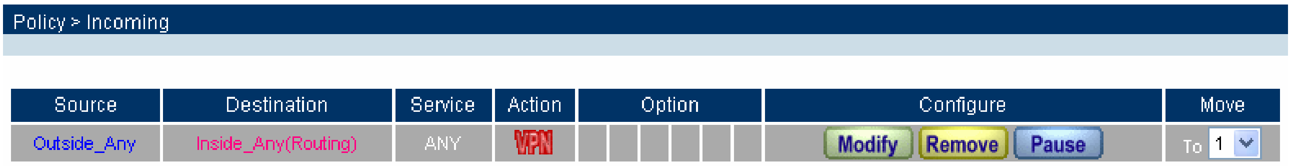
Outgoing Policy:



Policy > Outgoing

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	VPN		Modify Remove Pause	To 1
Inside_Any	Outside_Any	ANY	✓		Modify Remove Pause	To 2

Incoming Policy:



Policy > Incoming

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Inside_Any(Routing)	ANY	VPN		Modify Remove Pause	To 1

Example 2. Create a VPN connection between the Content Security Gateway and Windows XP Professional VPN Client.

Preparation Task:

Company A External IP is 210.66.155.90, Internal IP is 192.168.10.X

Remote User External IP is 210.66.155.91

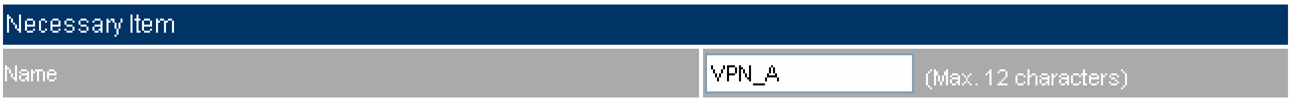
Remote user with an external IP wants to create a VPN connection with company A and connect to 192.168.10.100 for downloading the sharing file.

The Gateway of Company A is 192.168.10.1. The settings of company A are as the following.

Configuration of CS-500

Step 1. Enter the default IP of Company A's Content Security Gateway, 192.168.10.1. Click VPN in the menu bar on the left hand side, and then select the sub-select IPSec Autokey. Click Add.

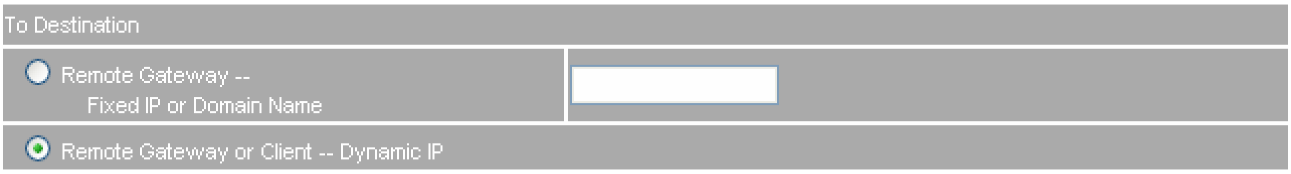
Step 2. Enter the VPN name, VPN_A in IPSec Autokey window.



Necessary Item

Name	VPN_A (Max. 12 characters)

Step 3. In to Destination table, choose Remote Gateway or Client – Dynamic IP.

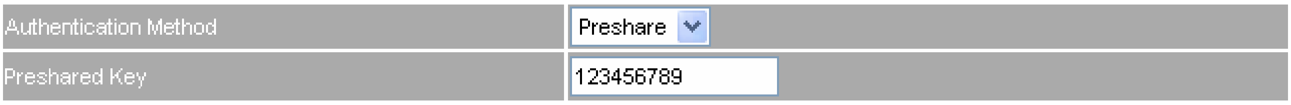


To Destination

○ Remote Gateway -- Fixed IP or Domain Name

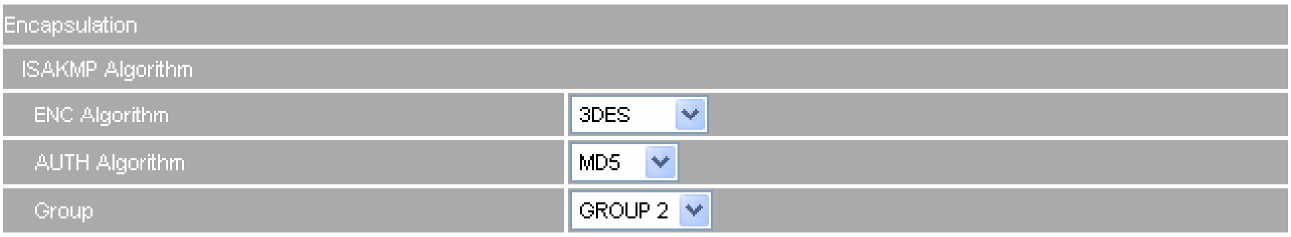
● Remote Gateway or Client -- Dynamic IP

Step 4. In Authentication Method Table enters the Preshared Key.



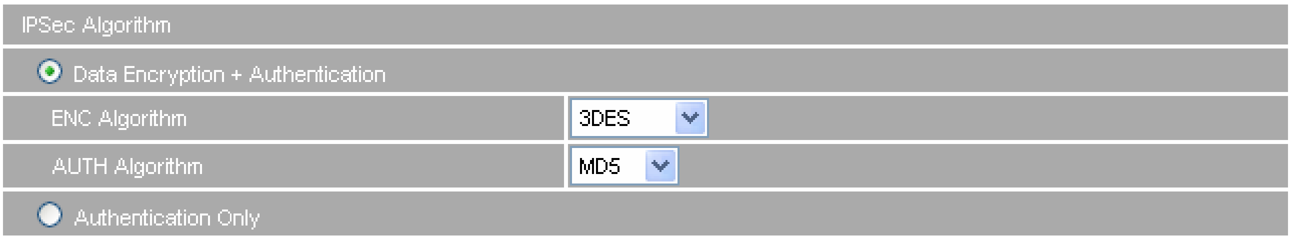
Authentication Method	Preshare
Preshared Key	123456789

Step 5. In Encapsulation or Authentication table, choose ISAKMP Algorithm. For communication via VPN, we choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm. And select Group 2 to connect.



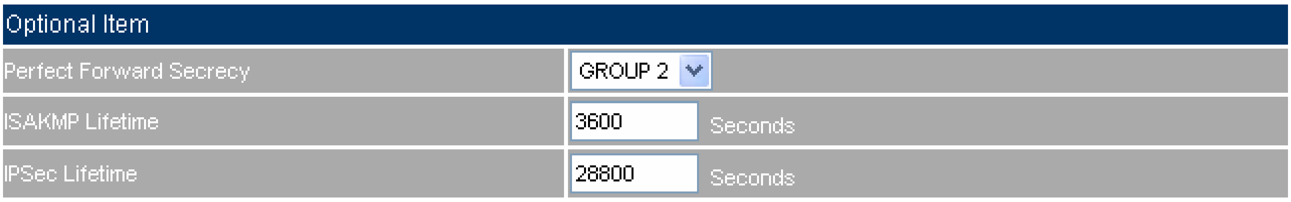
Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	3DES
AUTH Algorithm	MD5
Group	GROUP 2

Step 6. In IPSec Algorithm Table, choose Data Encryption + Authentication. We choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm.



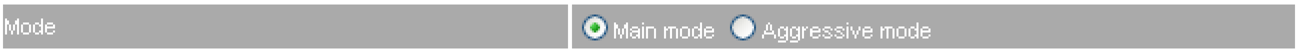
IPSec Algorithm	
● Data Encryption + Authentication	
ENC Algorithm	3DES
AUTH Algorithm	MD5
○ Authentication Only	

Step 7. Choose GROUP 2 as the Perfect Forward Secrecy setting, and leave the default setting with 28800 seconds in IPSec Lifetime and 3600 seconds for ISAKMP Lifetime.



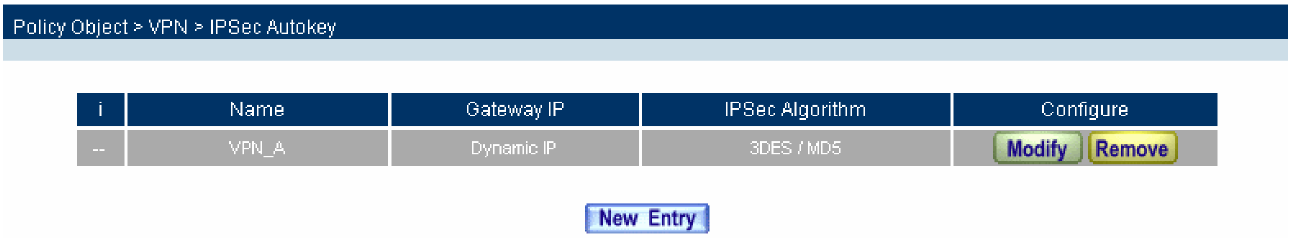
Optional Item	
Perfect Forward Secrecy	GROUP 2
ISAKMP Lifetime	3600 Seconds
IPSec Lifetime	28800 Seconds

Step 8. Select main mode as the algorithm.



Mode	● Main mode ○ Aggressive mode

Step 9. Click OK to finish the IPSec Aotukey setting of Company A.

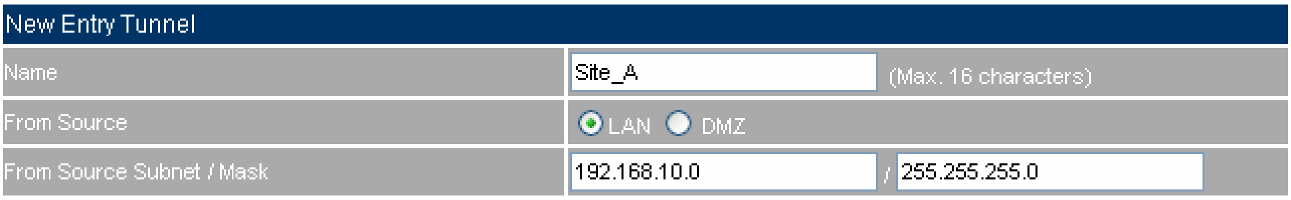


Policy Object > VPN > IPSec Autokey

i	Name	Gateway IP	IPSec Algorithm	Configure
--	VPN_A	Dynamic IP	3DES / MD5	Modify Remove

Step 10. Click Tunnel and press New Entry to configure the further setting.

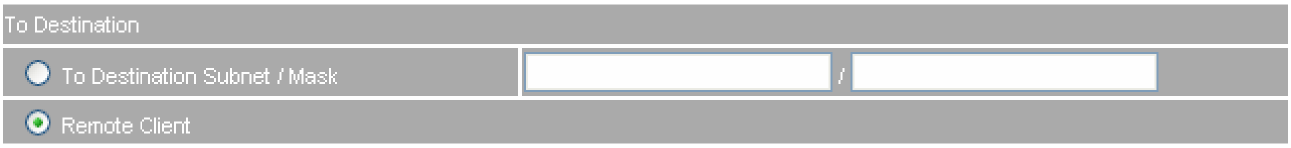
Step 11. Enter Site_A as the new tunnel name, and select LAN interface as the VPN source. Fill LAN IP subnet 192.168.10.0 with subnet mask IP 255.255.255.0.



New Entry Tunnel

Name	Site_A (Max. 16 characters)
From Source	● LAN ○ DMZ
From Source Subnet / Mask	192.168.10.0 / 255.255.255.0

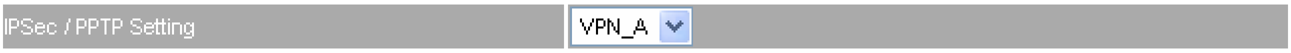
Step 12. In To Destination table, select Remote Client.



To Destination

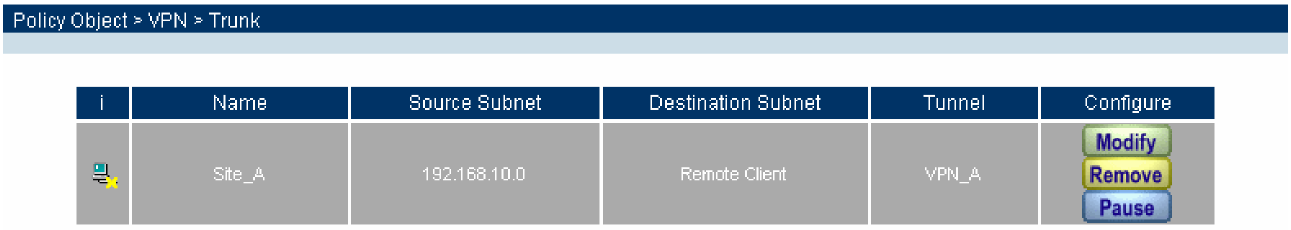
○ To Destination Subnet / Mask	/
● Remote Client	

Step 13. In IPSec / PPTP Setting, select VPN_A as the available tunnel.



IPSec / PPTP Setting	VPN_A

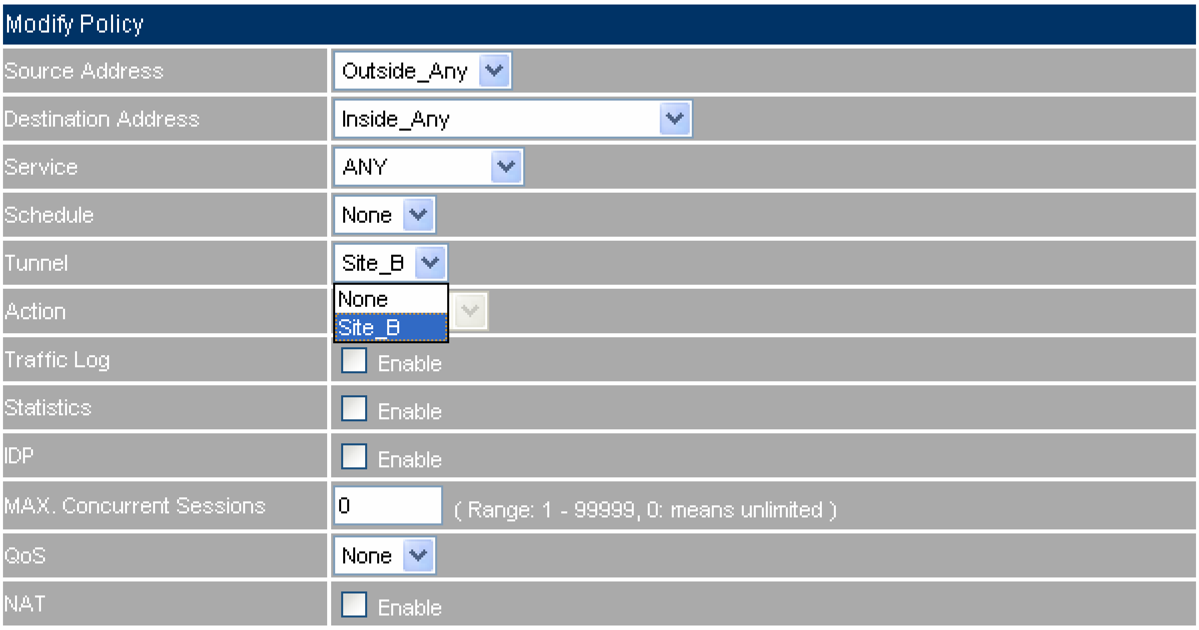
Step 14. Click OK to finish the Tunnel setting of Company A.



Policy Object > VPN > Trunk

i	Name	Source Subnet	Destination Subnet	Tunnel	Configure
	Site_A	192.168.10.0	Remote Client	VPN_A	Modify Remove Pause

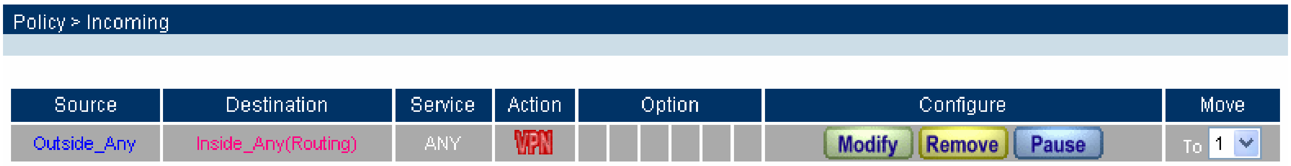
Step 15. Enable Tunnel setting in Incoming Policy.



Modify Policy

Source Address	Outside_Any
Destination Address	Inside_Any
Service	ANY
Schedule	None
Tunnel	Site_B None Site_B
Action	
Traffic Log	□ Enable
Statistics	□ Enable
IDP	□ Enable
MAX. Concurrent Sessions	0 (Range: 1 - 99999, 0: means unlimited)
QoS	None
NAT	□ Enable

Step 16. Click OK to finish the Policy setting of Company A.



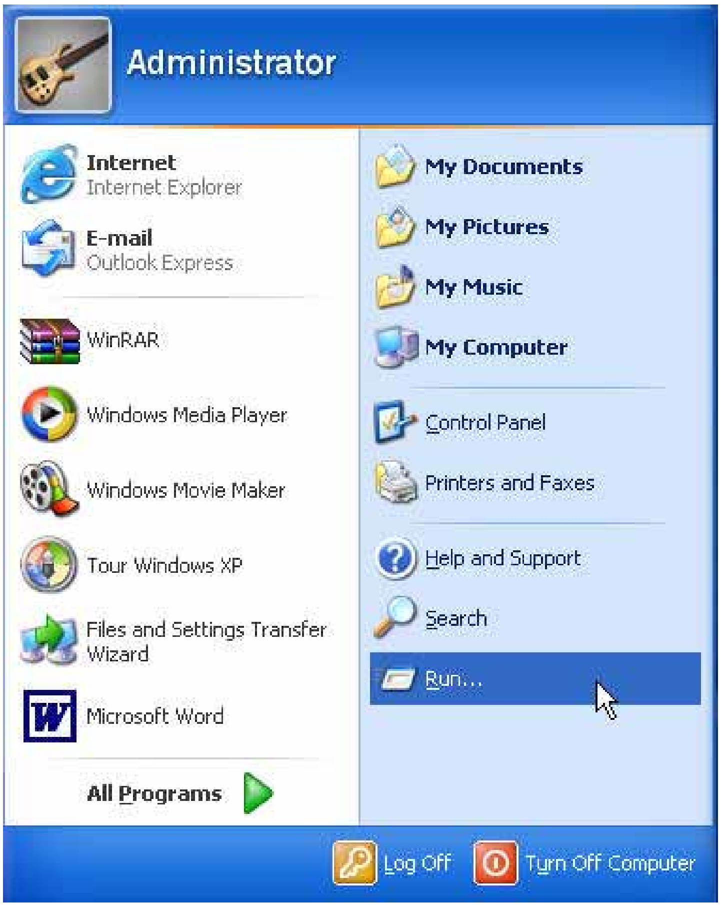
Policy > Incoming

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Inside_Any(Routing)	ANY	VPN		Modify Remove Pause	To 1

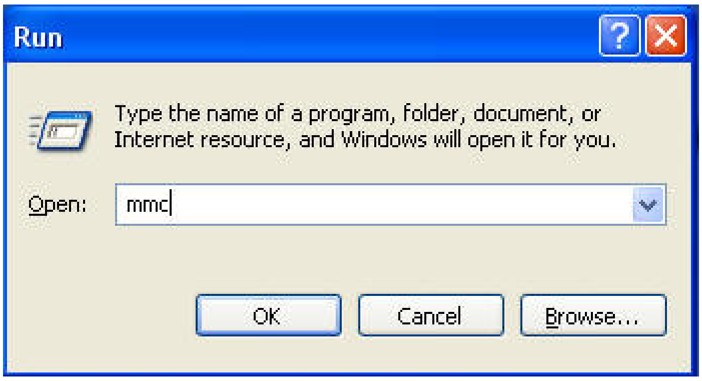
Configuration of WinXP

The IP of remote user is 210.66.155.91. The settings of remote user are as the following.

Step 1. Enter Windows XP, click Start and click Execute function.



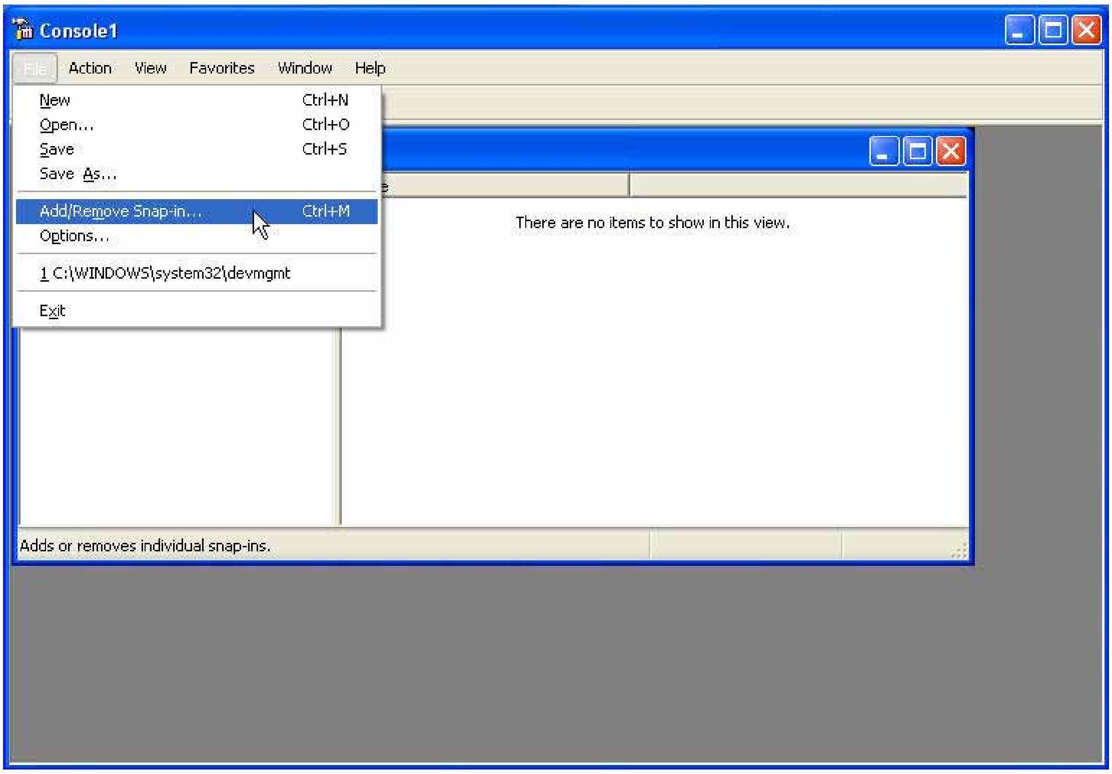
Step 2. In the Execute window, enter the command, mmc in Open.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: mmc

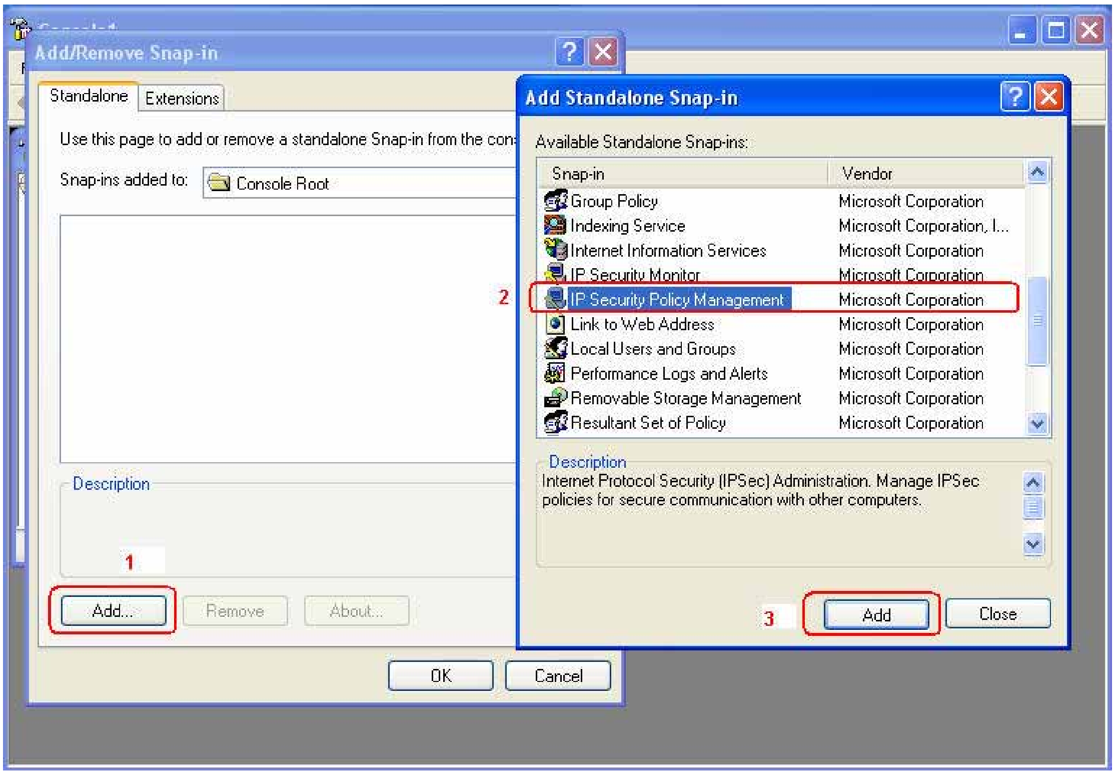
Step 3. Enter the Console window, click Console(C) option and click Add/Remove Embedded Management Option.



There are no items to show in this view.

Adds or removes individual snap-ins.

Step 4. Enter Add/Remove Embedded Management Option window and click Add. In Add/ Remove Embedded Management Option window, click Add to add Create IP Security Policy.



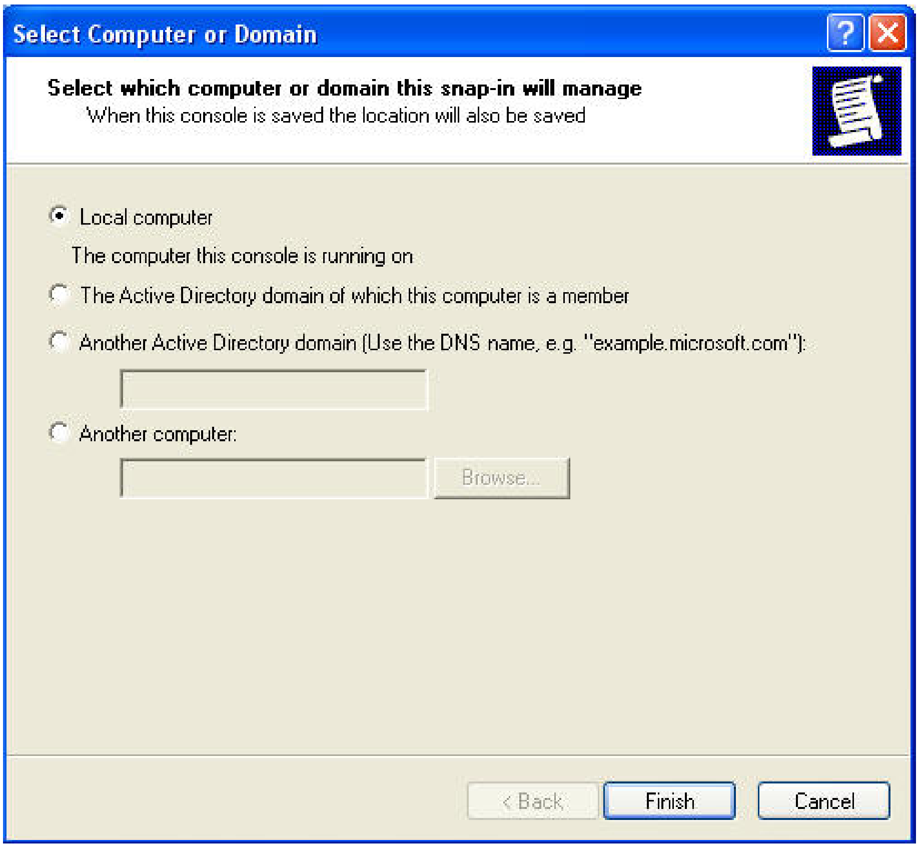
Use this page to add or remove a standalone Snap-in from the con

Available Standalone Snap-ins:

Snap-in	Vendor
Group Policy	Microsoft Corporation
Indexing Service	Microsoft Corporation, I...
Internet Information Services	Microsoft Corporation
IP Security Monitor	Microsoft Corporation
IP Security Policy Management	Microsoft Corporation
Link to Web Address	Microsoft Corporation
Local Users and Groups	Microsoft Corporation
Performance Logs and Alerts	Microsoft Corporation
Removable Storage Management	Microsoft Corporation
Resultant Set of Policy	Microsoft Corporation

Description
Internet Protocol Security (IPSec) Administration. Manage IPSec policies for secure communication with other computers.

Step 5. Choose Local Machine (L) for finishing the setting of Add.



Select which computer or domain this snap-in will manage

When this console is saved the location will also be saved

● Local computer

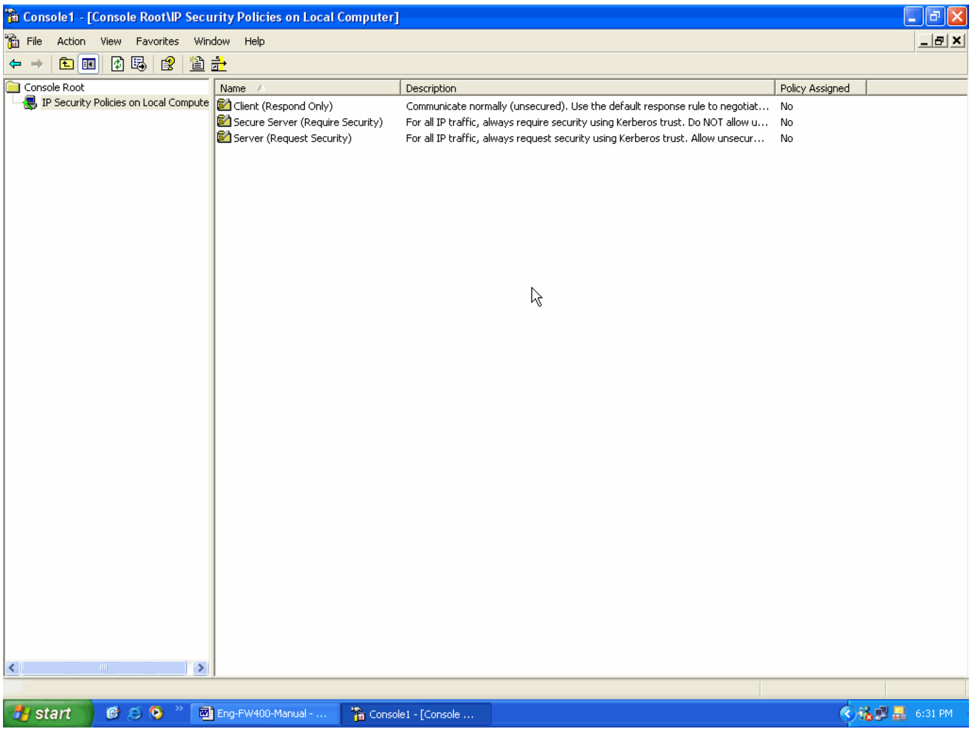
The computer this console is running on

○ The Active Directory domain of which this computer is a member

○ Another Active Directory domain (Use the DNS name, e.g. "example.microsoft.com"):

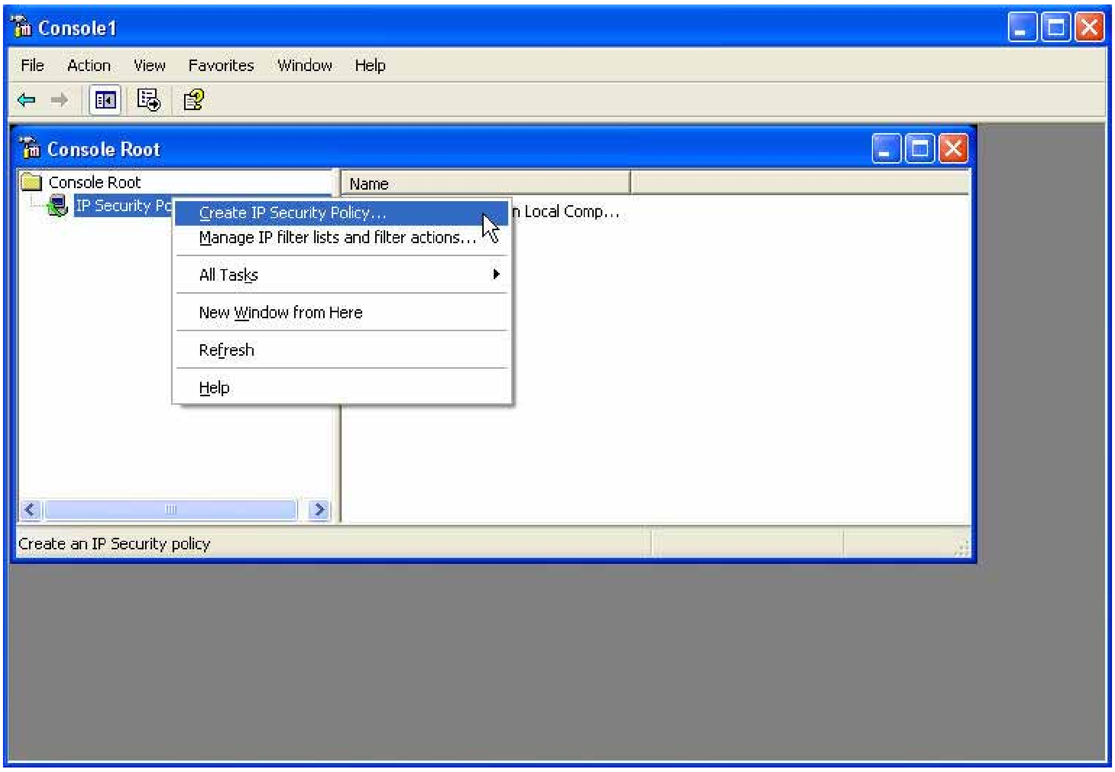
○ Another computer:

Step 6. Finish the setting of Add.

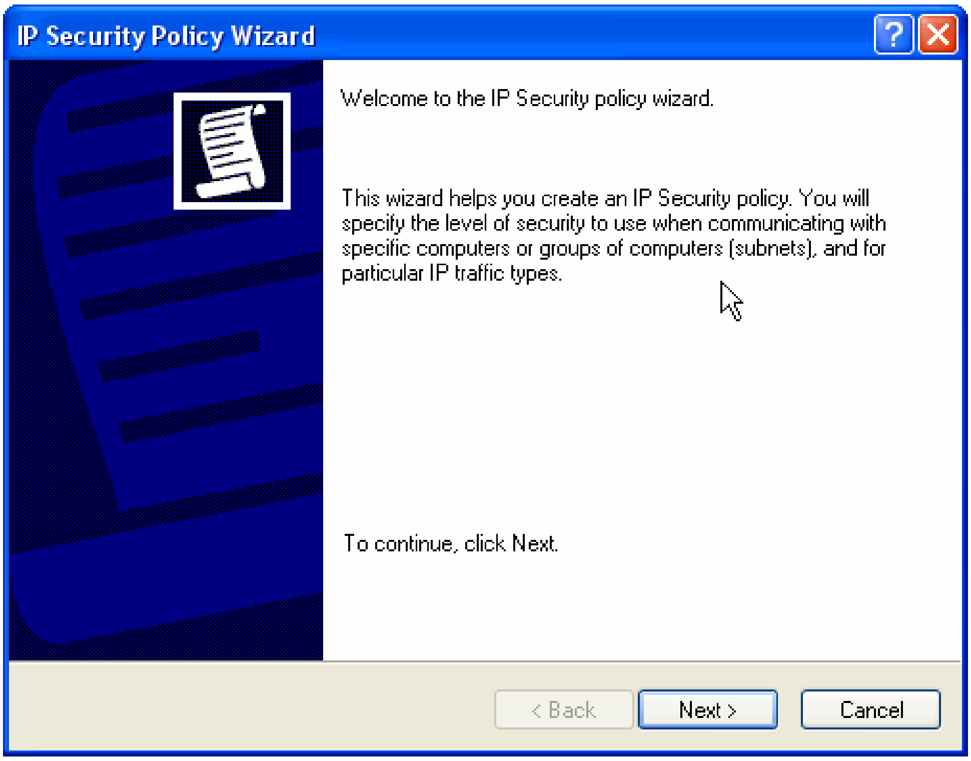


Name	Description	Policy Assigned
Client (Respond Only)	Communicate normally (unsecured). Use the default response rule to negotiat...	No
Secure Server (Require Security)	For all IP traffic, always require security using Kerberos trust. Do NOT allow u...	No
Server (Request Security)	For all IP traffic, always request security using Kerberos trust. Allow unsecur...	No

Step 7. Click the right button of mouse in IP Security Policies on Local Machine and choose Create IP Security Policy(C) option.


Console1
File Action View Favorites Window Help
Console Root
Console Root
IP Security Po
Name
n Local Comp...
Create IP Security Policy...
Manage IP filter lists and filter actions...
All Tasks
New Window from Here
Refresh
Help
Create an IP Security policy

Step 8. Click Next.

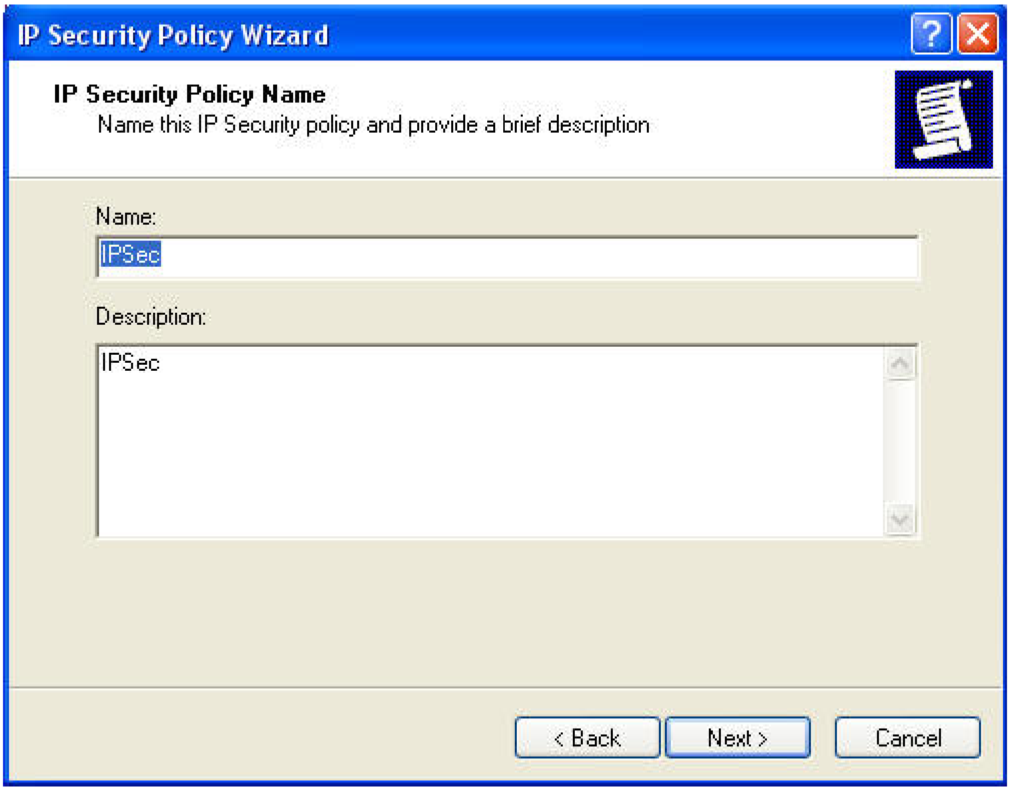


Welcome to the IP Security policy wizard.

This wizard helps you create an IP Security policy. You will specify the level of security to use when communicating with specific computers or groups of computers (subnets), and for particular IP traffic types.

To continue, click Next.

Step 9. Enter the Name of this VPN and optionally give it a brief description.



IP Security Policy Wizard

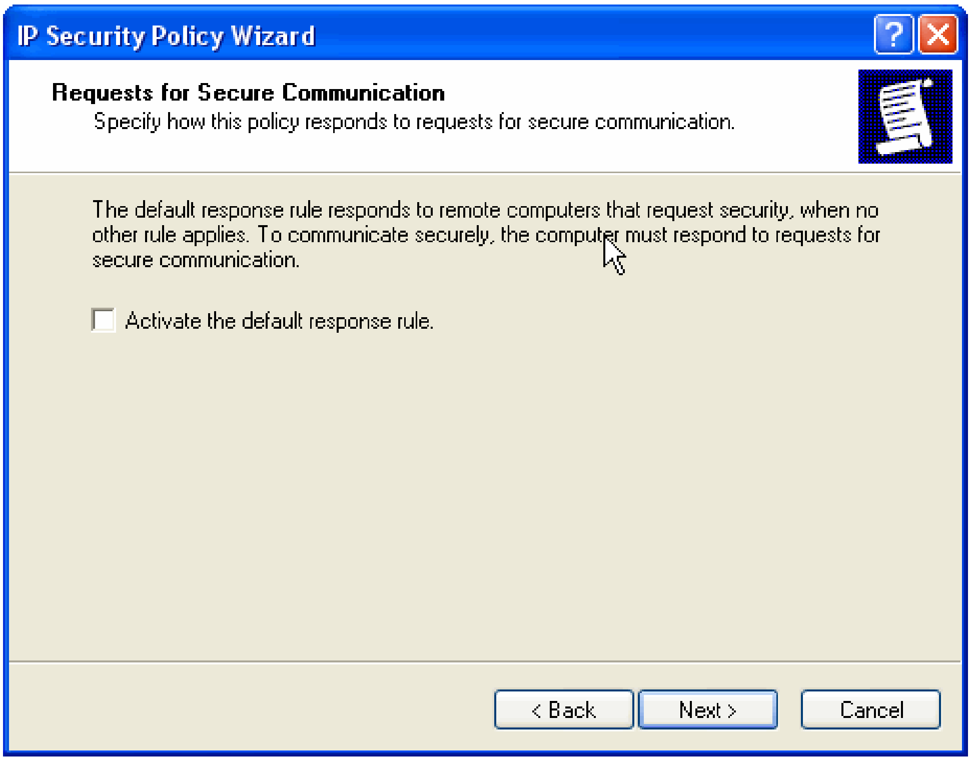
IP Security Policy Name

Name this IP Security policy and provide a brief description

Name: IPSec

Description: IPSec

Step 10. Disable **Activate the default response rule**. And click Next.



IP Security Policy Wizard

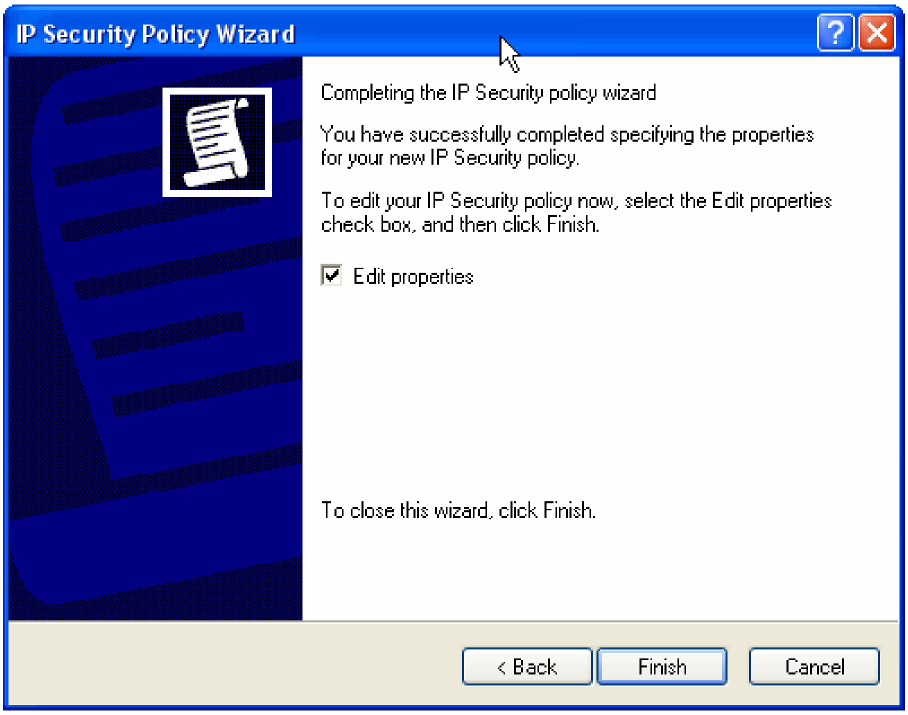
Requests for Secure Communication

Specify how this policy responds to requests for secure communication.

The default response rule responds to remote computers that request security, when no other rule applies. To communicate securely, the computer must respond to requests for secure communication.

☐ Activate the default response rule.

Step 11. Completing the IP Security Policy setting and click Finish. Enable Edit properties.



IP Security Policy Wizard

Completing the IP Security policy wizard

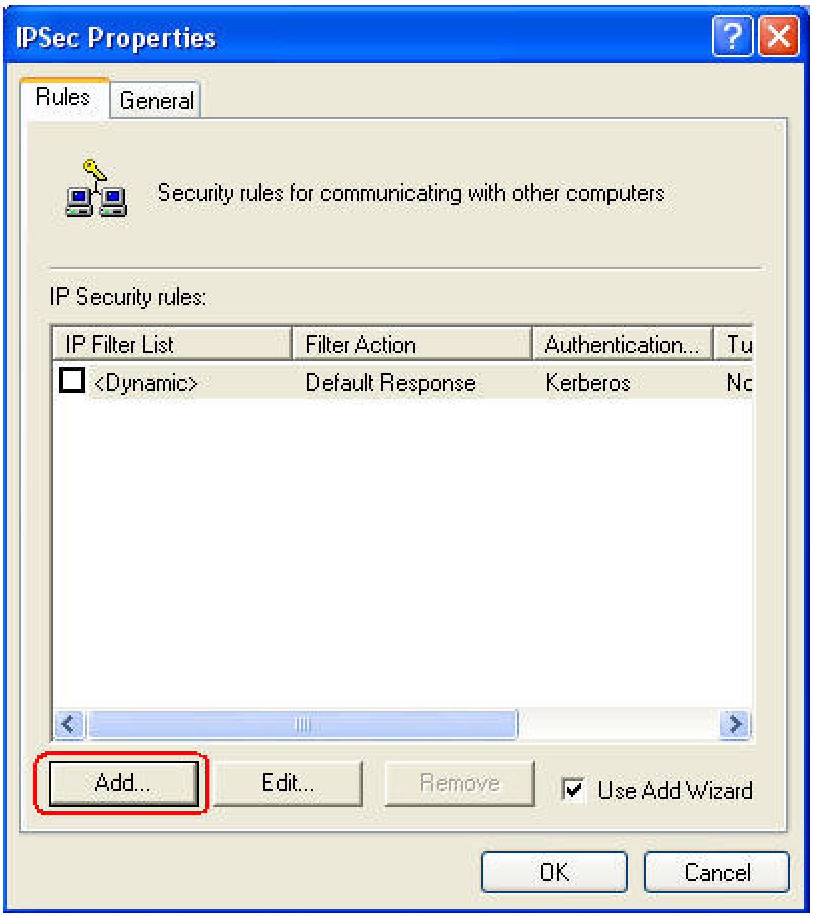
You have successfully completed specifying the properties for your new IP Security policy.

To edit your IP Security policy now, select the Edit properties check box, and then click Finish.

☑ Edit properties

To close this wizard, click Finish.

Step 12. In window, click Add and click Use Add Wizard.



IPSec Properties

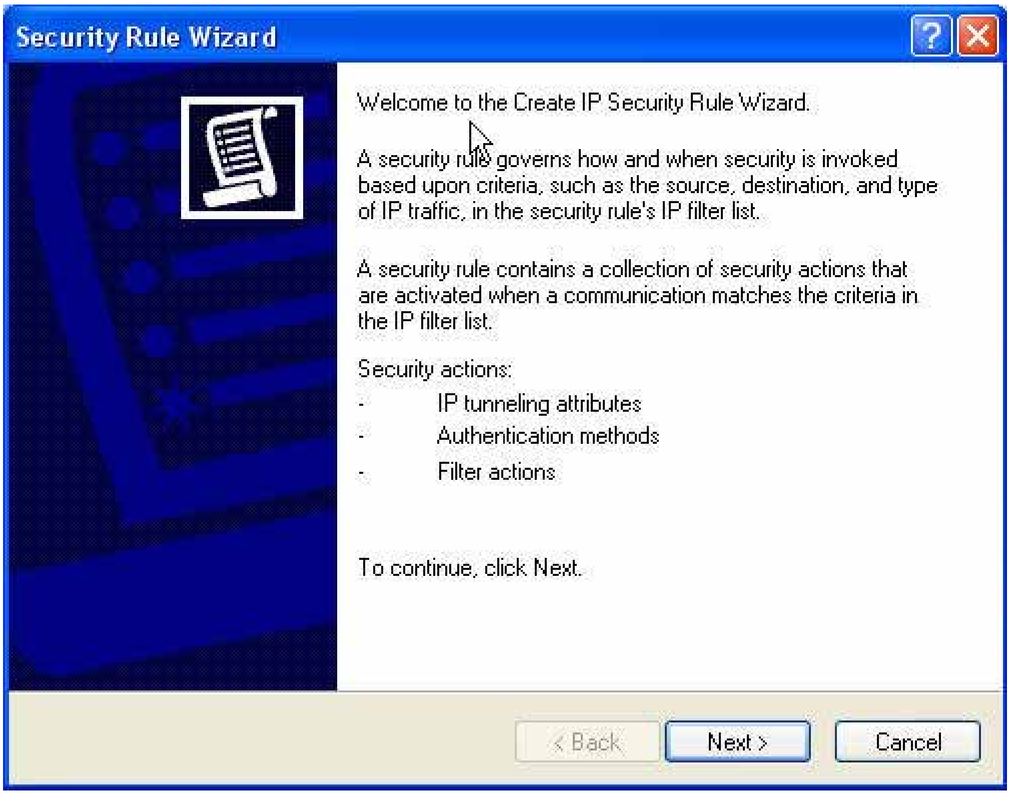
Security rules for communicating with other computers

IP Security rules:

IP Filter List	Filter Action	Authentication...	Tu
□ <Dynamic>	Default Response	Kerberos	Nc

☑ Use Add Wizard

Step 13. Click next.



Security Rule Wizard

Welcome to the Create IP Security Rule Wizard.

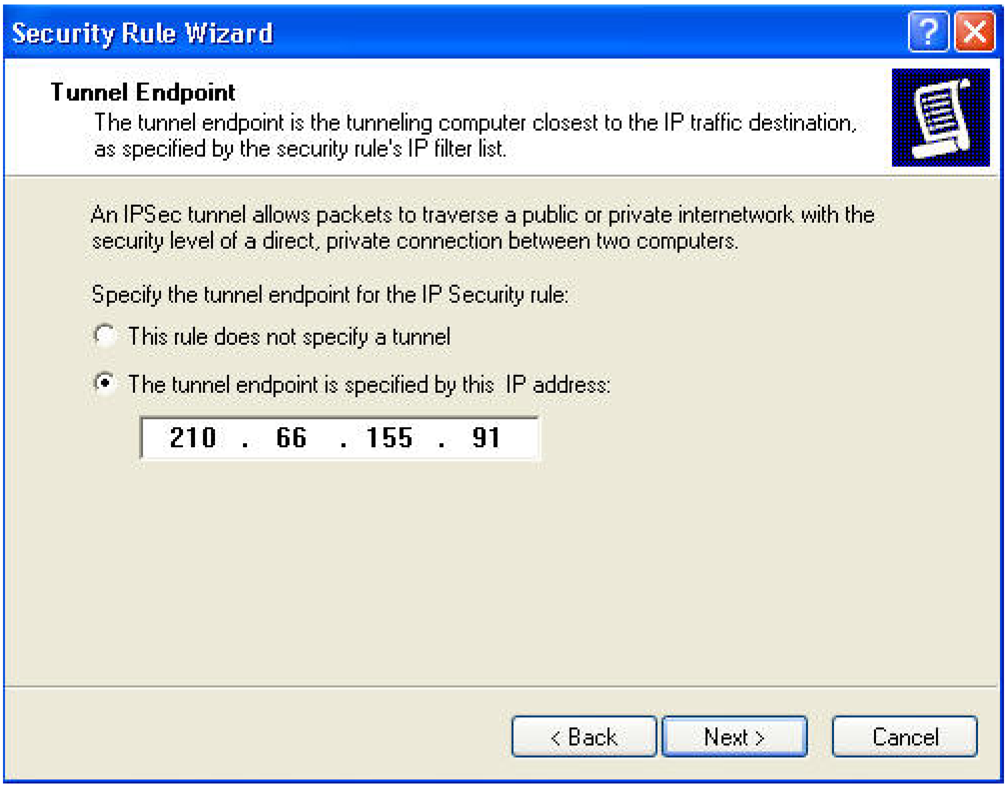
A security rule governs how and when security is invoked based upon criteria, such as the source, destination, and type of IP traffic, in the security rule's IP filter list.

A security rule contains a collection of security actions that are activated when a communication matches the criteria in the IP filter list.

Security actions:
- IP tunneling attributes
- Authentication methods
- Filter actions

To continue, click Next.

Step 14. Enter the WAN IP of Remote user, 210.66.155.91.



Security Rule Wizard

Tunnel Endpoint
The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the security rule's IP filter list.

An IPSec tunnel allows packets to traverse a public or private internetwork with the security level of a direct, private connection between two computers.

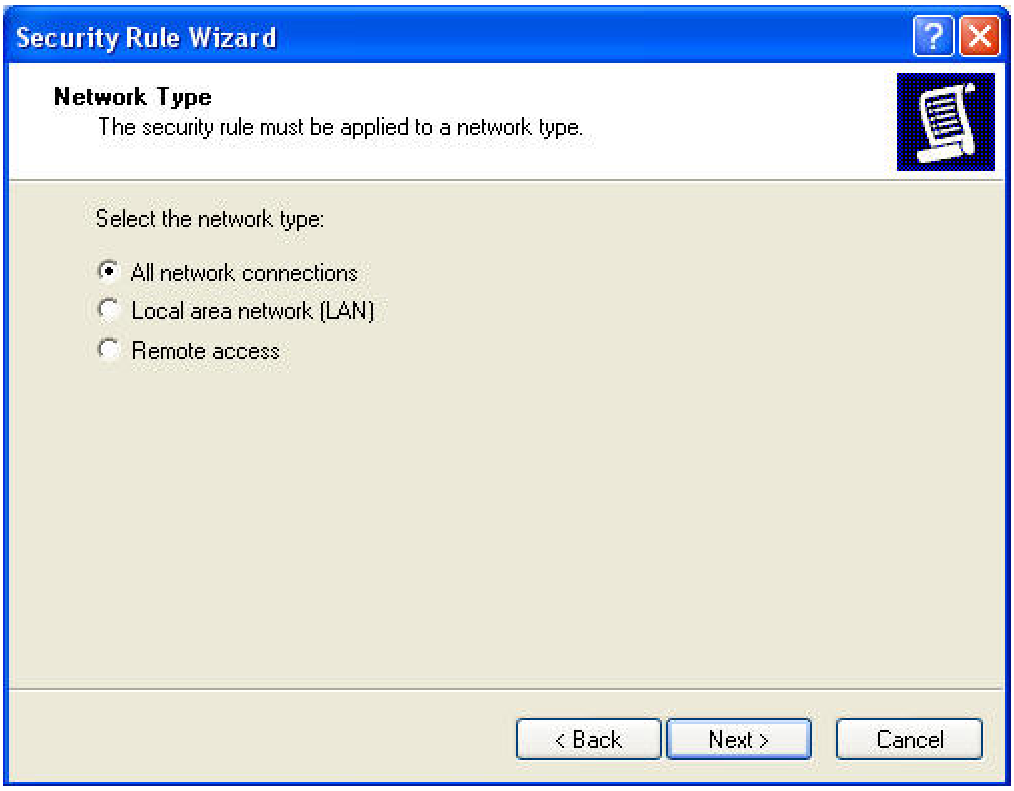
Specify the tunnel endpoint for the IP Security rule:

○ This rule does not specify a tunnel

● The tunnel endpoint is specified by this IP address:

210 . 66 . 155 . 91

Step 15. click all network connections.



Security Rule Wizard

Network Type

The security rule must be applied to a network type.

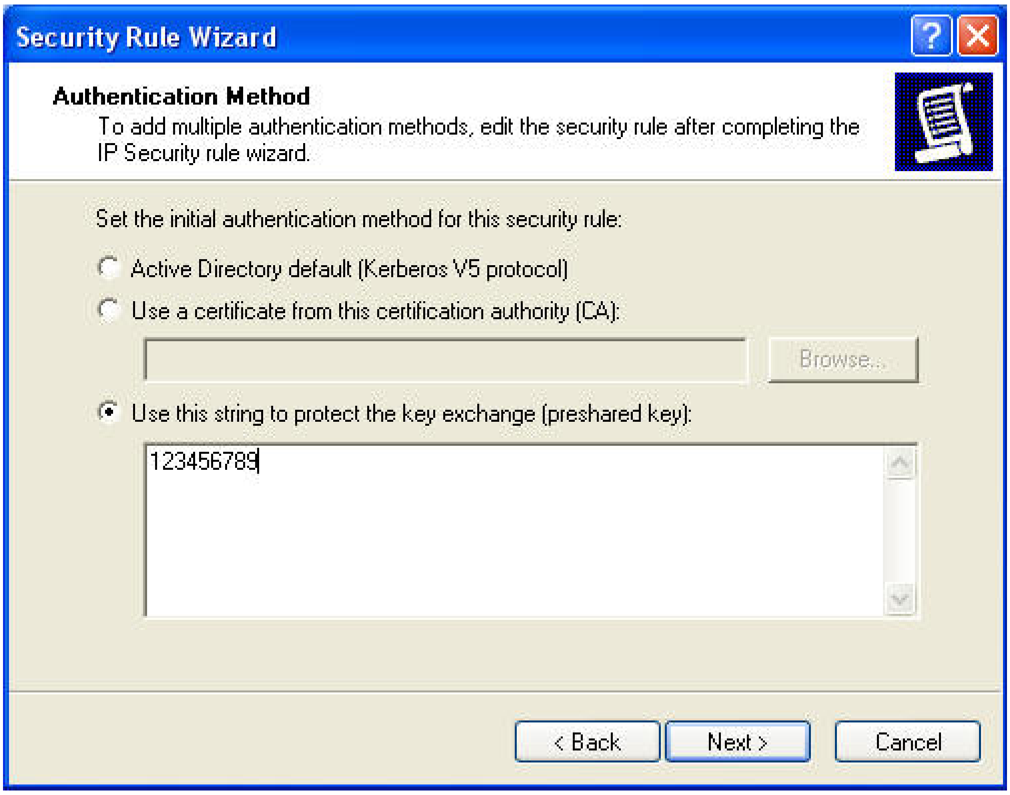
Select the network type:

● All network connections

○ Local area network (LAN)

○ Remote access

Step 16. Choose Use this string to protect the key exchange (Preshared Key). And enter the key, 123456789.



Security Rule Wizard

Authentication Method

To add multiple authentication methods, edit the security rule after completing the IP Security rule wizard.

Set the initial authentication method for this security rule:

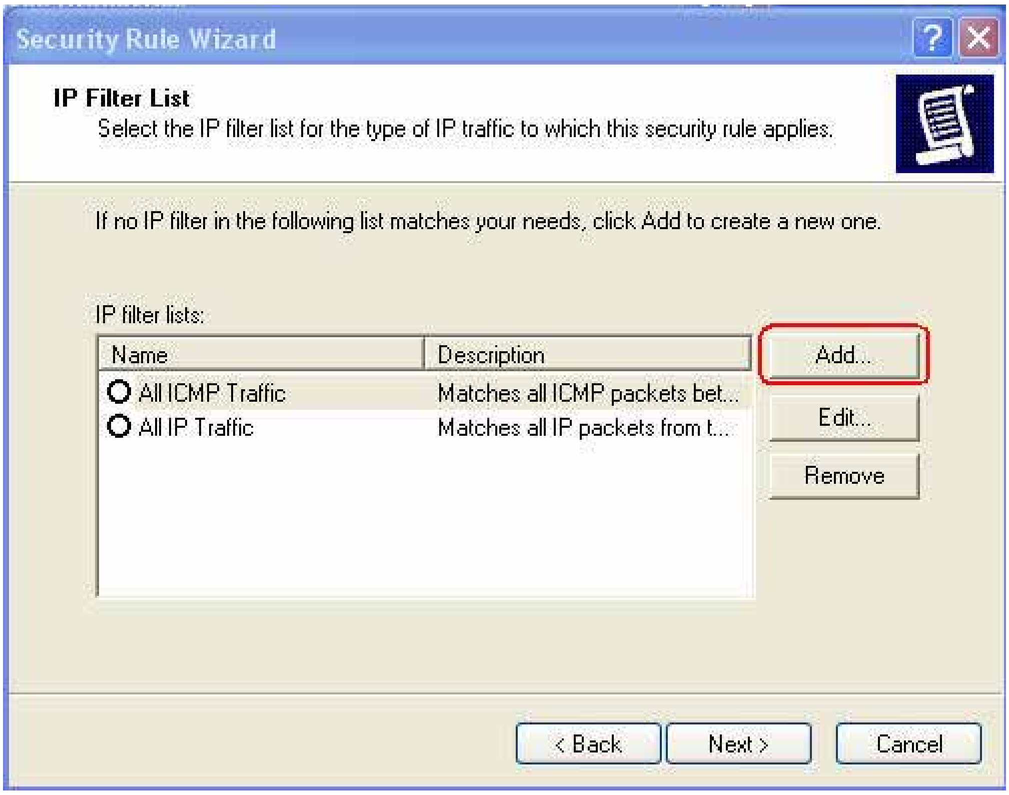
○ Active Directory default (Kerberos V5 protocol)

○ Use a certificate from this certification authority (CA):

● Use this string to protect the key exchange (preshared key):

123456789

Step 17. Click Add.



Security Rule Wizard

IP Filter List

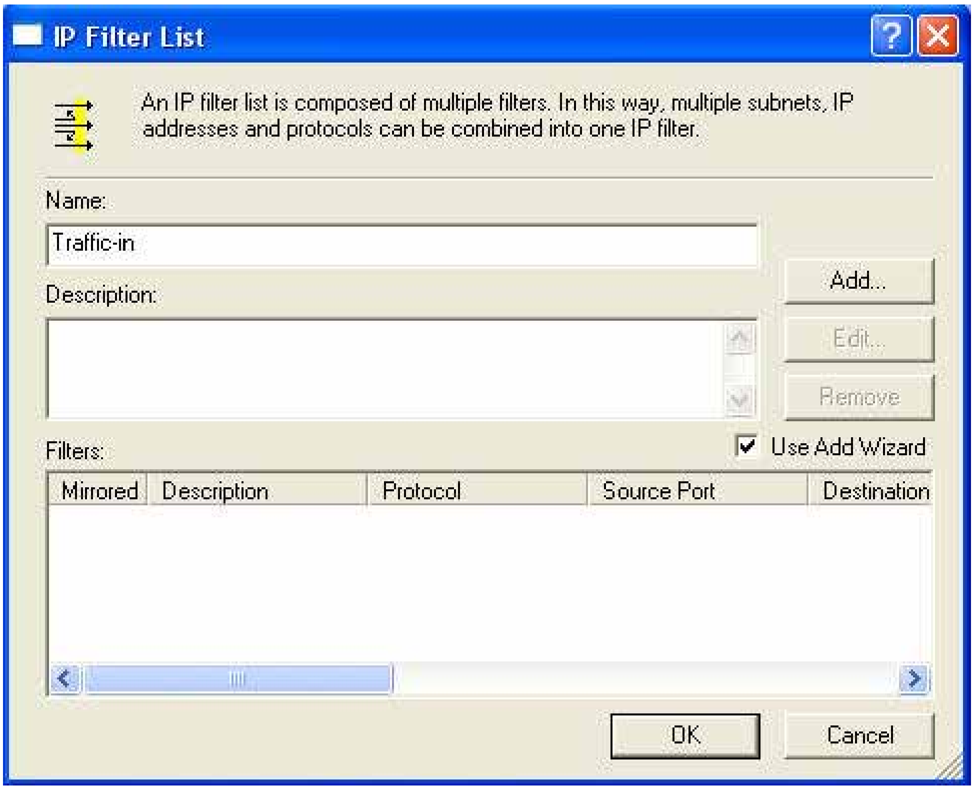
Select the IP filter list for the type of IP traffic to which this security rule applies.

If no IP filter in the following list matches your needs, click Add to create a new one.

IP filter lists:

Name	Description
○ All ICMP Traffic	Matches all ICMP packets bet...
○ All IP Traffic	Matches all IP packets from t...

Step 18. Enter the name of IP filter and click "Add..".



IP Filter List

An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter.

Name:

Traffic-in

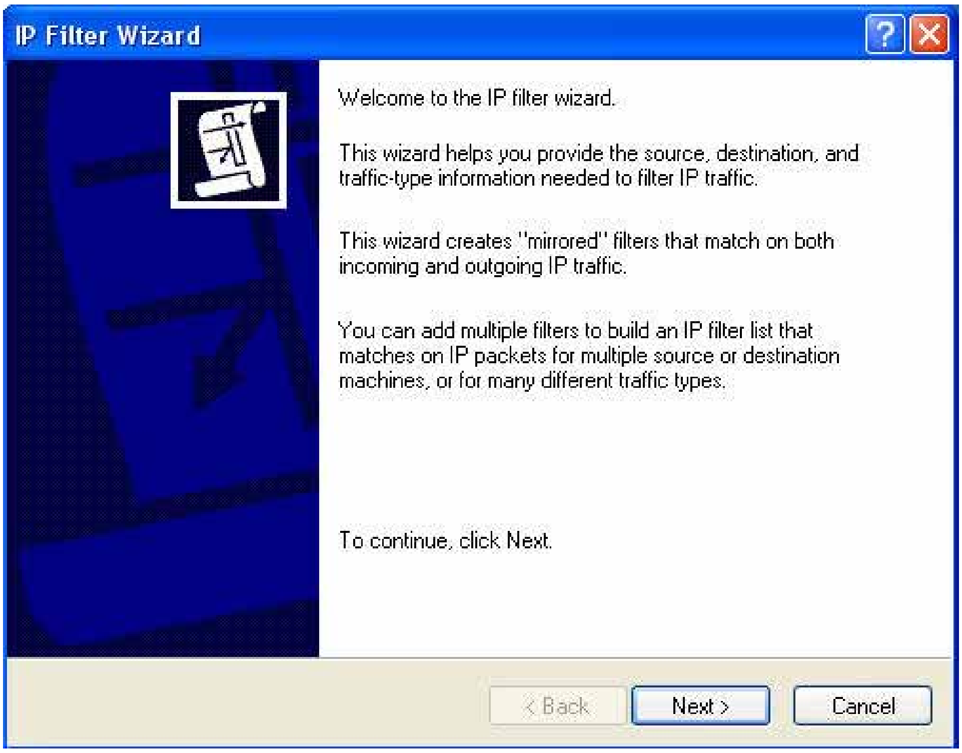
Description:

☑ Use Add Wizard

Filters:

Mirrored	Description	Protocol	Source Port	Destination

Step 19. Click next.



Welcome to the IP filter wizard.

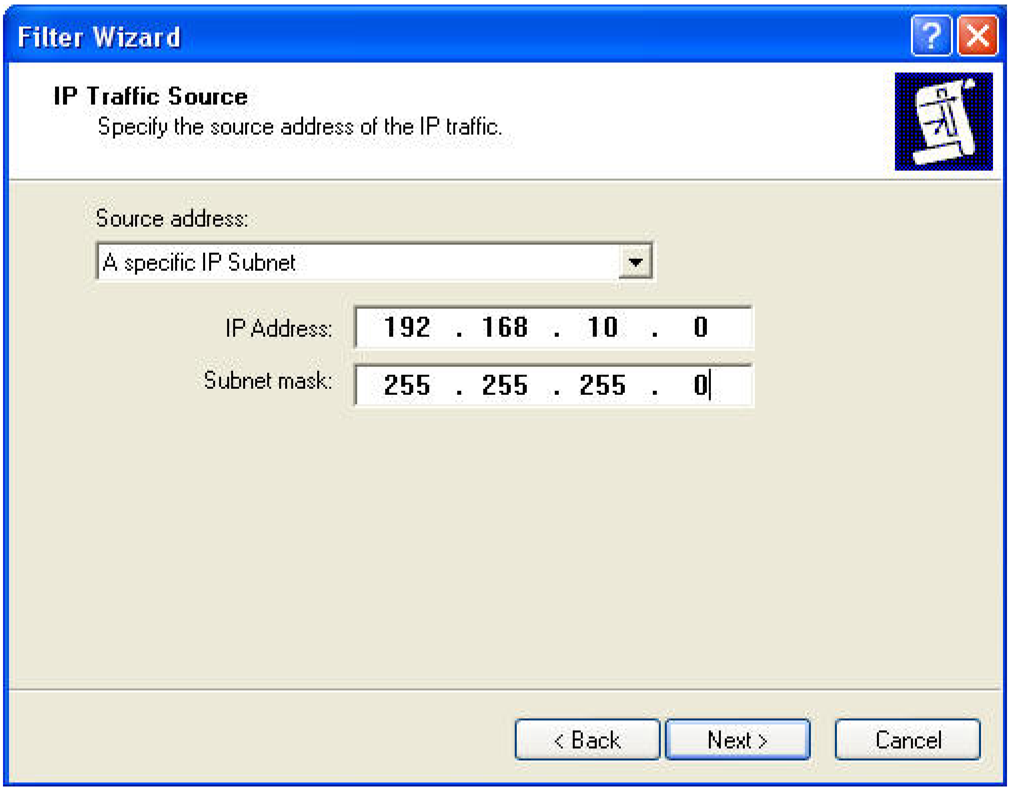
This wizard helps you provide the source, destination, and traffic-type information needed to filter IP traffic.

This wizard creates "mirrored" filters that match on both incoming and outgoing IP traffic.

You can add multiple filters to build an IP filter list that matches on IP packets for multiple source or destination machines, or for many different traffic types.

To continue, click Next.

Step 20. In Source address, click down the arrow to select the specific IP Subnet and fill Company A's IP Address, 192.168.10.0 and Subnet mask 255.255.255.0.



IP Traffic Source

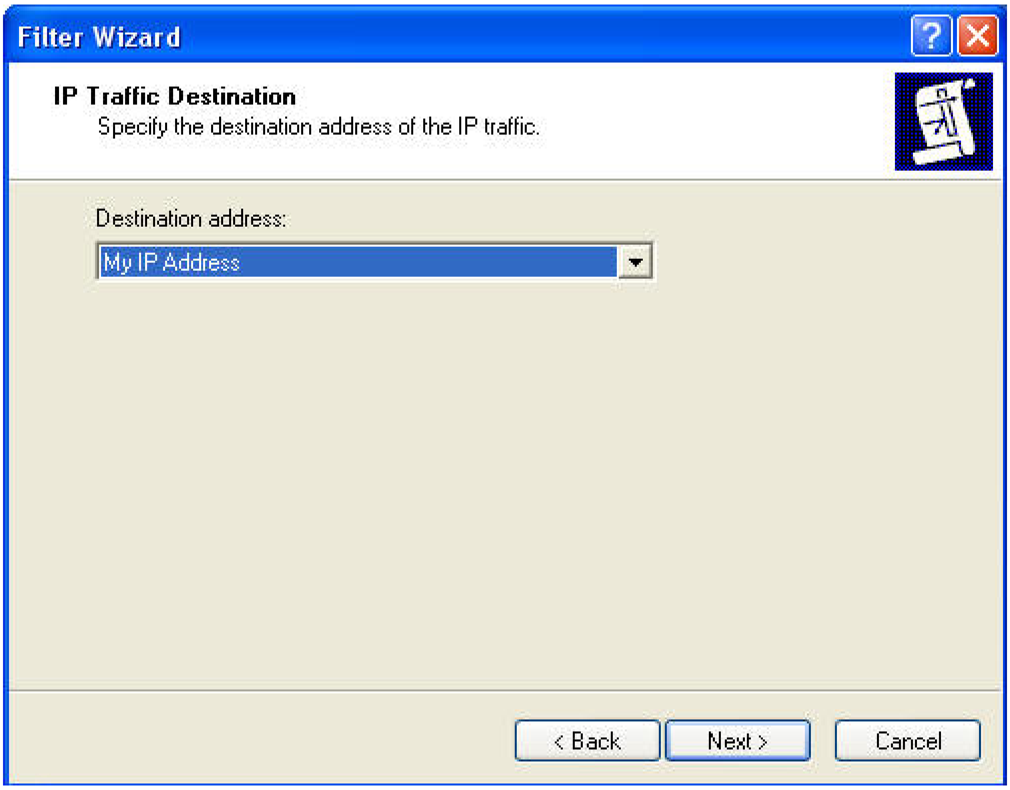
Specify the source address of the IP traffic.

Source address: A specific IP Subnet

IP Address: 192 . 168 . 10 . 0

Subnet mask: 255 . 255 . 255 . 0

Step 21. In Destination address, click down the arrow to select the My IP Address.



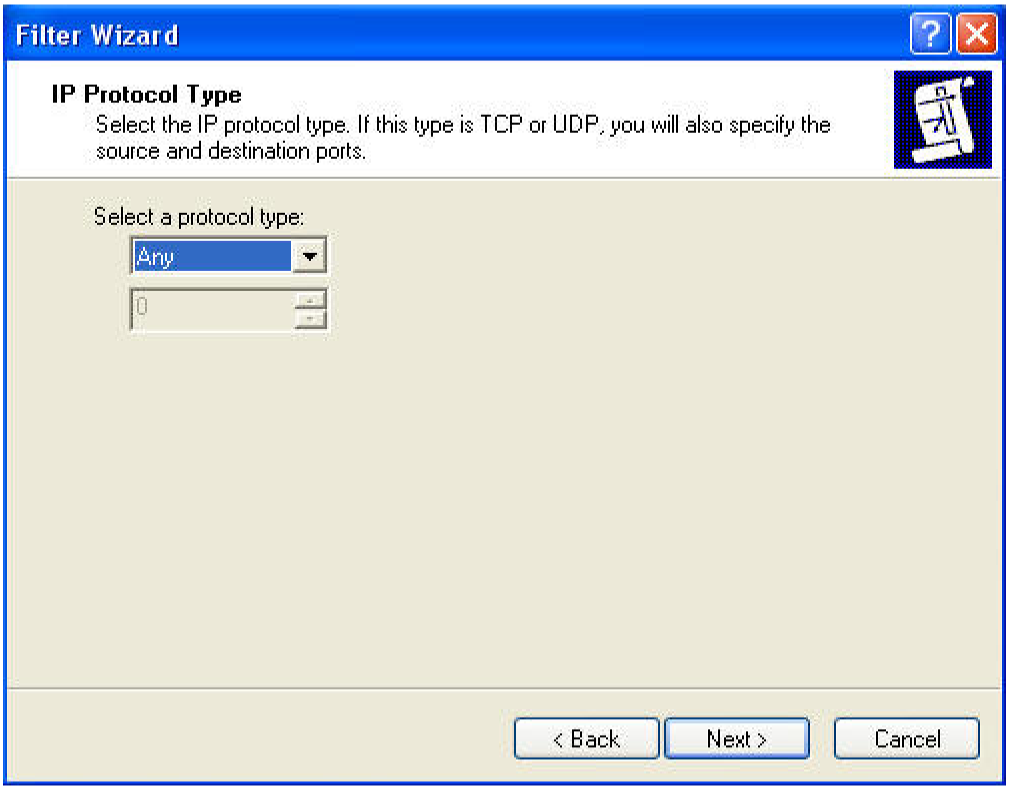
Filter Wizard

IP Traffic Destination

Specify the destination address of the IP traffic.

Destination address: My IP Address

Step 22. Click next.



Filter Wizard

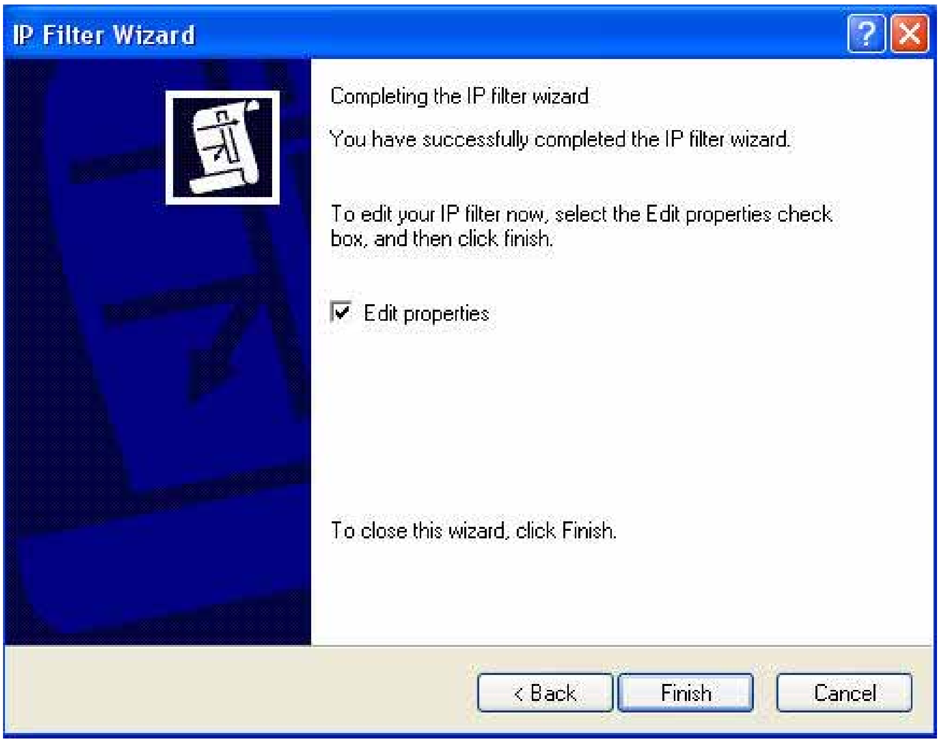
IP Protocol Type

Select the IP protocol type. If this type is TCP or UDP, you will also specify the source and destination ports.

Select a protocol type: Any

0

Step 23. Please enable edit properties, and click finish.



Completing the IP filter wizard

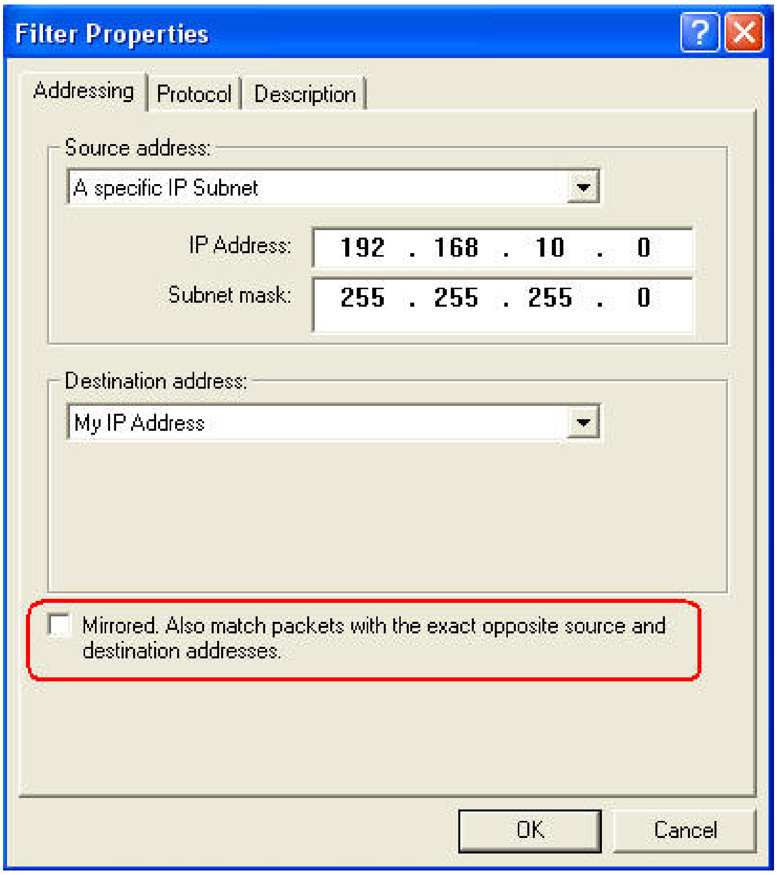
You have successfully completed the IP filter wizard.

To edit your IP filter now, select the Edit properties check box, and then click finish.

☑ Edit properties

To close this wizard, click Finish.

Step 24. Please don't enable Mirrored, and click OK.



Source address:

A specific IP Subnet

IP Address: 192 . 168 . 10 . 0

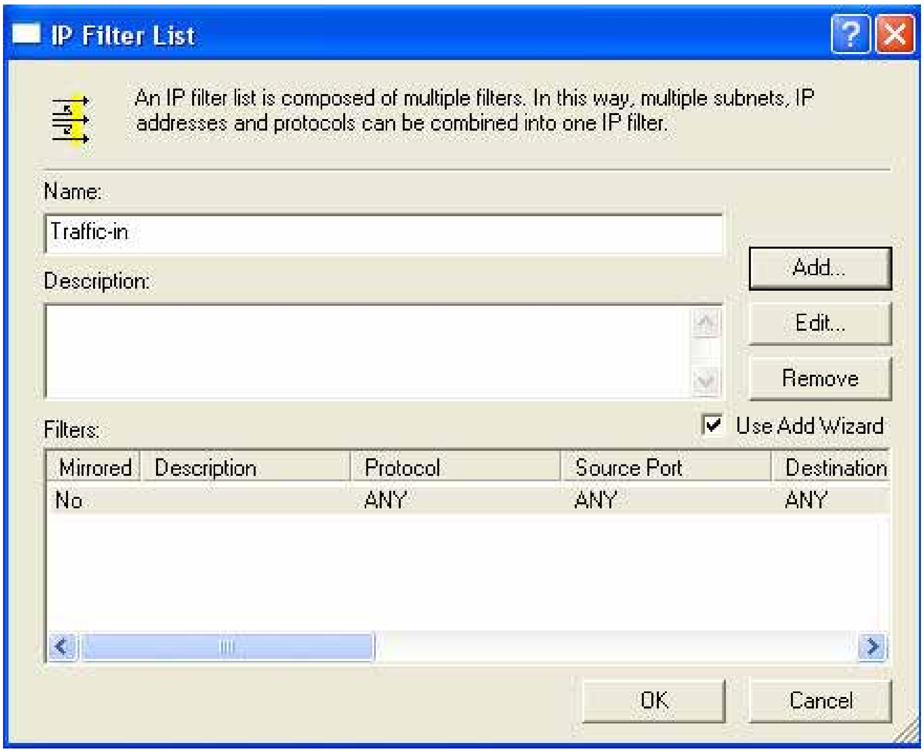
Subnet mask: 255 . 255 . 255 . 0

Destination address:

My IP Address

☐ Mirrored. Also match packets with the exact opposite source and destination addresses.

Step 25. Click OK.



IP Filter List

An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter.

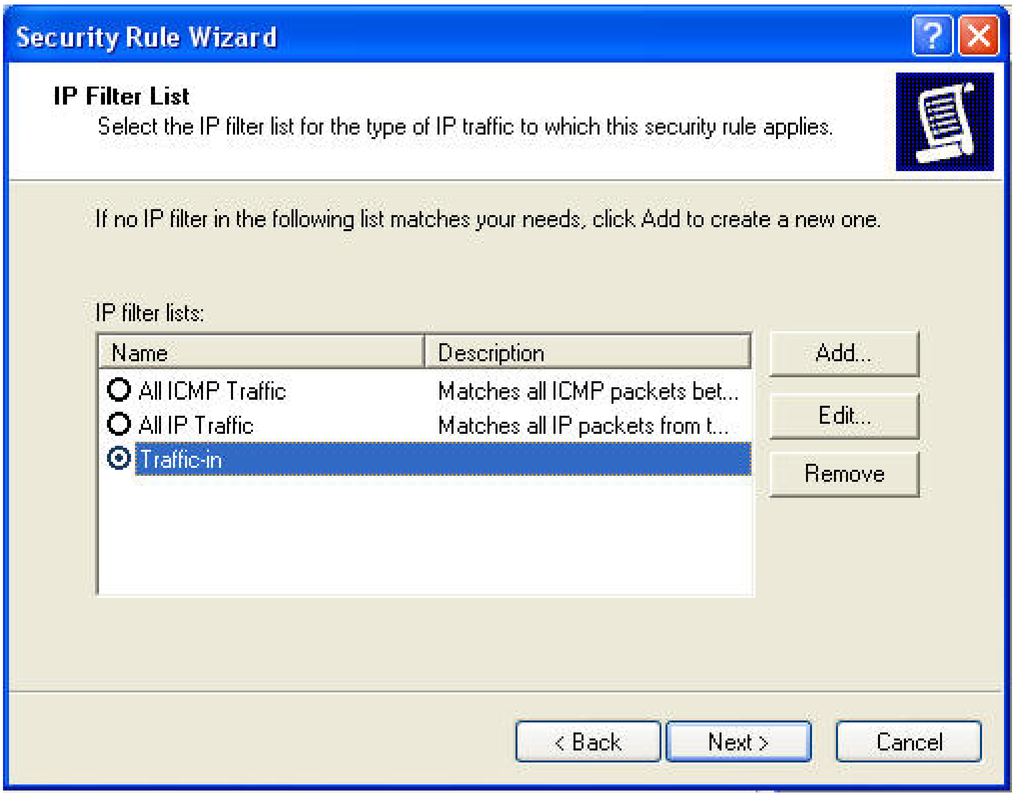
Name: Traffic-in

Description:

Filters: ☑ Use Add Wizard

Mirrored	Description	Protocol	Source Port	Destination
No		ANY	ANY	ANY

Step 26. Select Traffic-in and click next.



Security Rule Wizard

IP Filter List

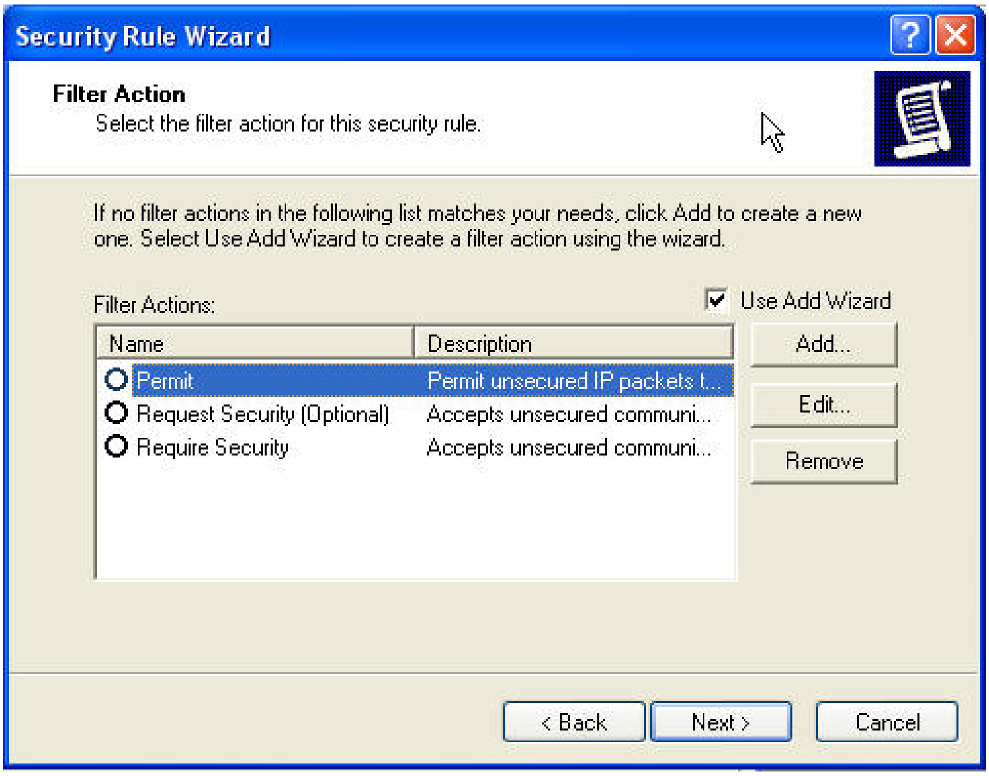
Select the IP filter list for the type of IP traffic to which this security rule applies.

If no IP filter in the following list matches your needs, click Add to create a new one.

IP filter lists:

Name	Description
○ All ICMP Traffic	Matches all ICMP packets bet...
○ All IP Traffic	Matches all IP packets from t...
● Traffic-in	

Step 27. Enable User Add Wizard and click add.



Filter Action

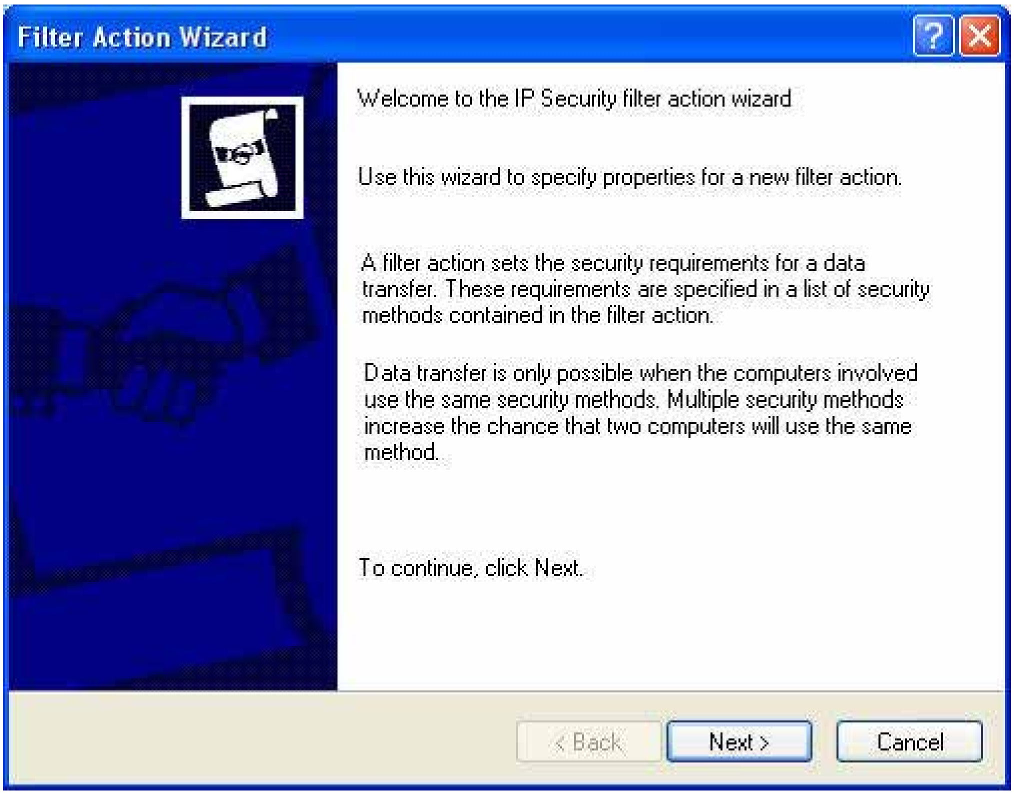
Select the filter action for this security rule.

If no filter actions in the following list matches your needs, click Add to create a new one. Select Use Add Wizard to create a filter action using the wizard.

Filter Actions: ☑ Use Add Wizard

Name	Description
○ Permit	Permit unsecured IP packets t...
○ Request Security (Optional)	Accepts unsecured communi...
○ Require Security	Accepts unsecured communi...

Step 28. Click next.



Welcome to the IP Security filter action wizard

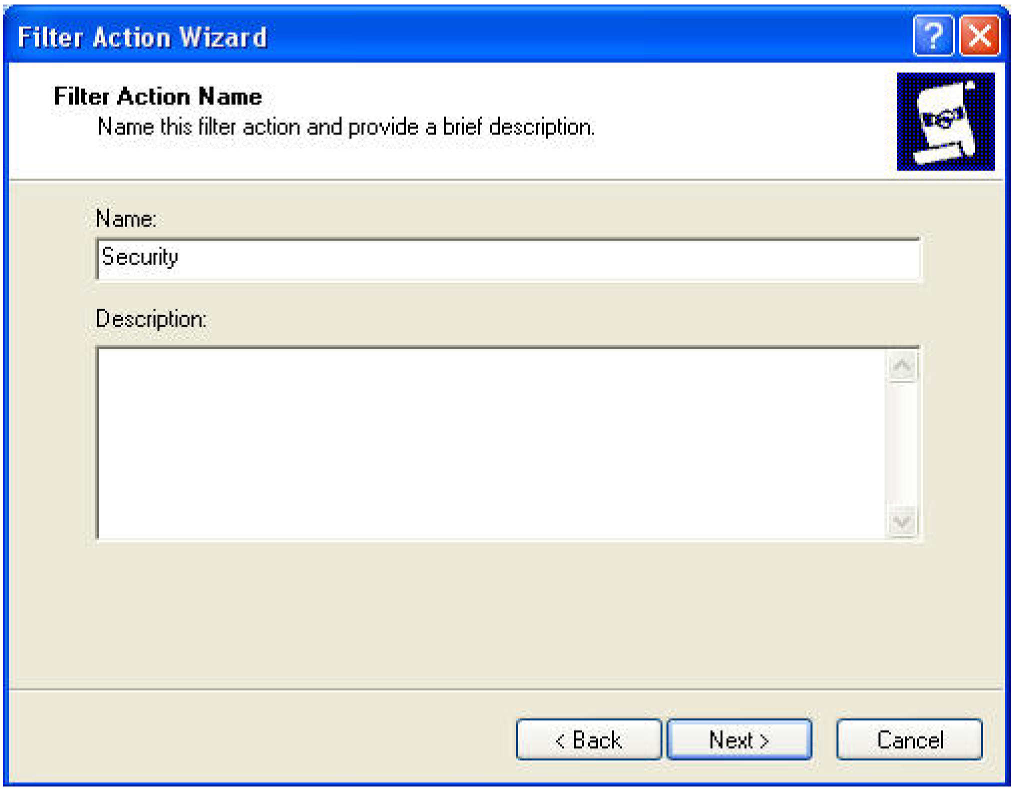
Use this wizard to specify properties for a new filter action.

A filter action sets the security requirements for a data transfer. These requirements are specified in a list of security methods contained in the filter action.

Data transfer is only possible when the computers involved use the same security methods. Multiple security methods increase the chance that two computers will use the same method.

To continue, click Next.

Step 29. Enter the name of filter action and click next.



Filter Action Wizard

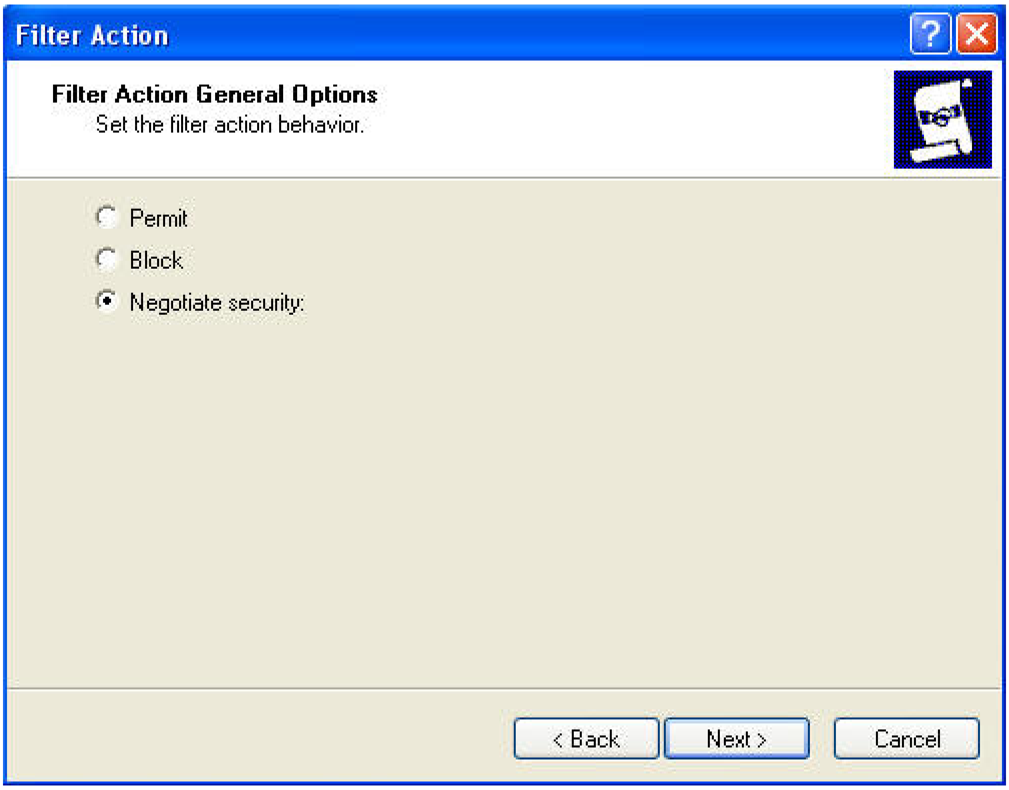
Filter Action Name

Name this filter action and provide a brief description.

Name: Security

Description:

Step 30. Select Negotiate security and click next.



Filter Action

Filter Action General Options

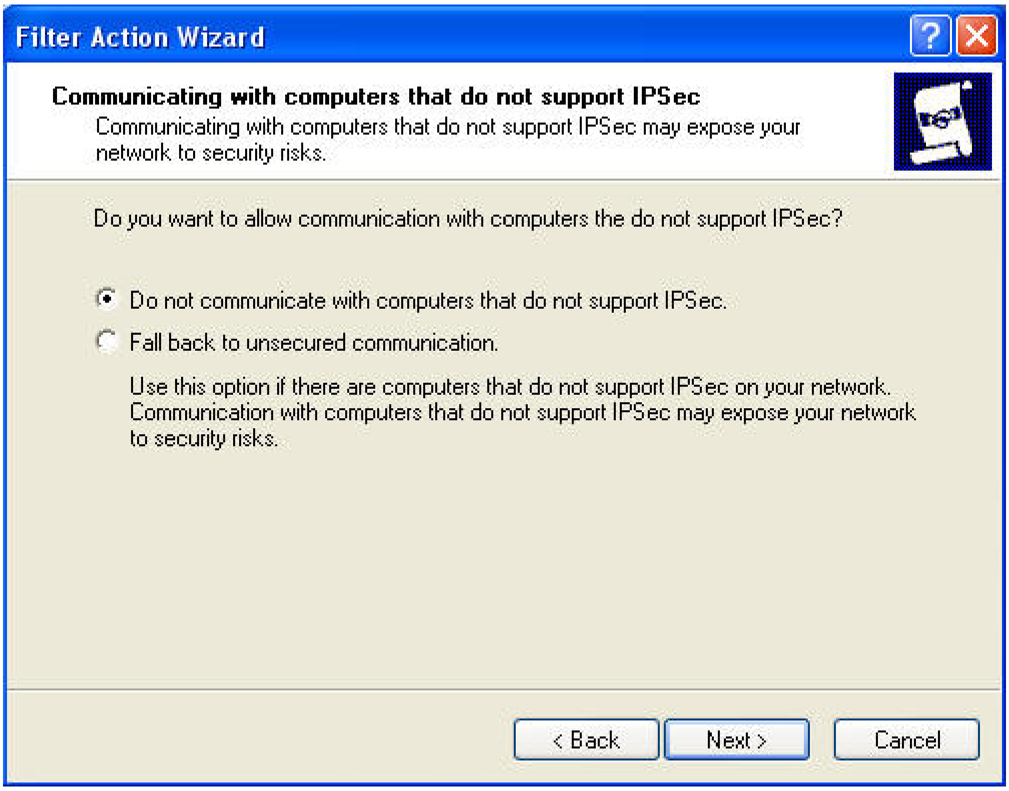
Set the filter action behavior.

○ Permit

○ Block

● Negotiate security:

Step 31. Click next.



Communicating with computers that do not support IPSec

Communicating with computers that do not support IPSec may expose your network to security risks.

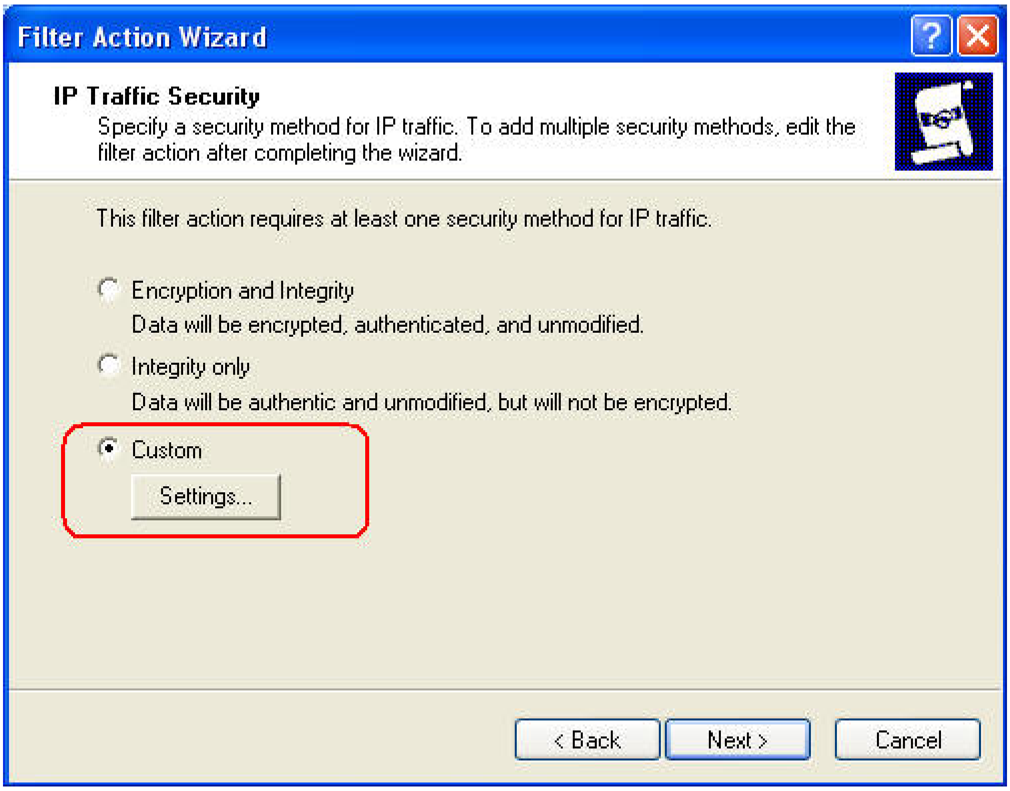
Do you want to allow communication with computers the do not support IPSec?

● Do not communicate with computers that do not support IPSec.

○ Fall back to unsecured communication.

Use this option if there are computers that do not support IPSec on your network. Communication with computers that do not support IPSec may expose your network to security risks.

Step 32. Select Custom and click settings.



IP Traffic Security

Specify a security method for IP traffic. To add multiple security methods, edit the filter action after completing the wizard.

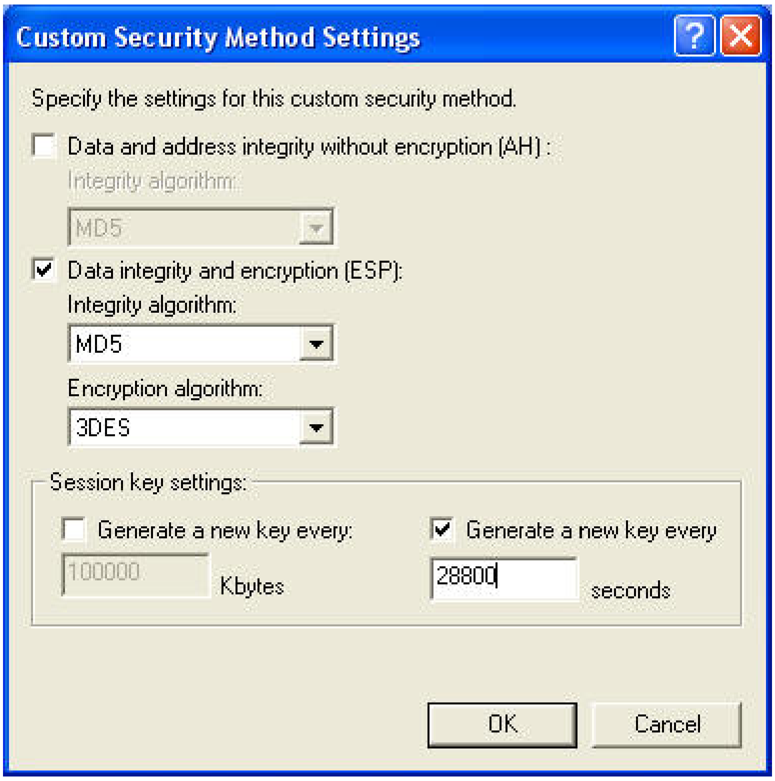
This filter action requires at least one security method for IP traffic.

○ Encryption and Integrity
Data will be encrypted, authenticated, and unmodified.

○ Integrity only
Data will be authentic and unmodified, but will not be encrypted.

● Custom

Step 33. Click Data Integrity and Encapsulation and choose MD5 and 3DES. Click Generate a New key after every 28800 seconds. And click 3 times OK to return.



Custom Security Method Settings

Specify the settings for this custom security method.

□ Data and address integrity without encryption (AH) :

Integrity algorithm: MD5

☑ Data integrity and encryption (ESP):

Integrity algorithm: MD5

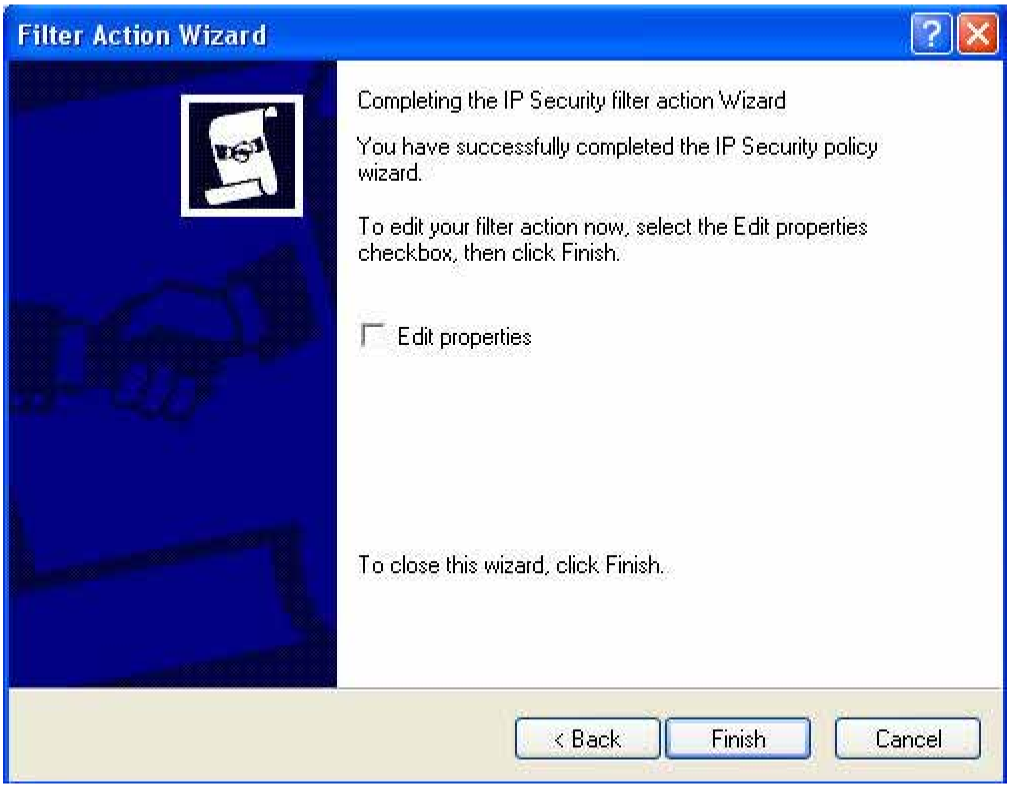
Encryption algorithm: 3DES

Session key settings:

□ Generate a new key every: 100000 Kbytes

☑ Generate a new key every 28800 seconds

Step 34. Click finish.



Filter Action Wizard

Completing the IP Security filter action Wizard

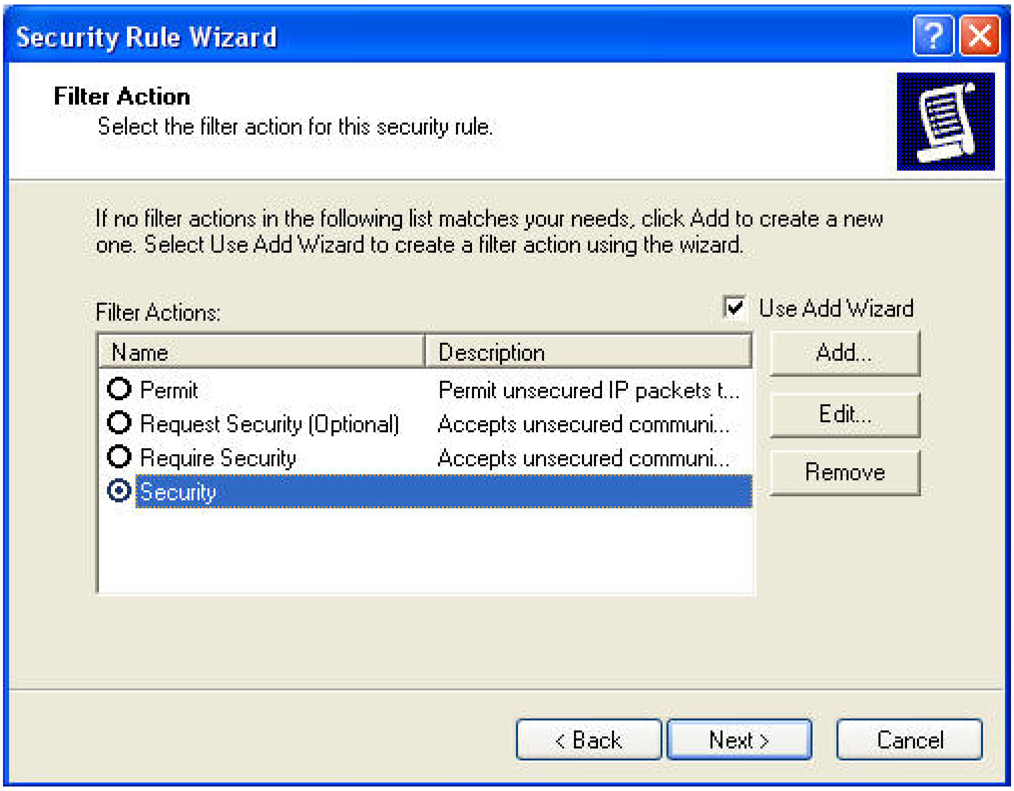
You have successfully completed the IP Security policy wizard.

To edit your filter action now, select the Edit properties checkbox, then click Finish.

□ Edit properties

To close this wizard, click Finish.

Step 35. Select security and click next.



Security Rule Wizard

Filter Action

Select the filter action for this security rule.

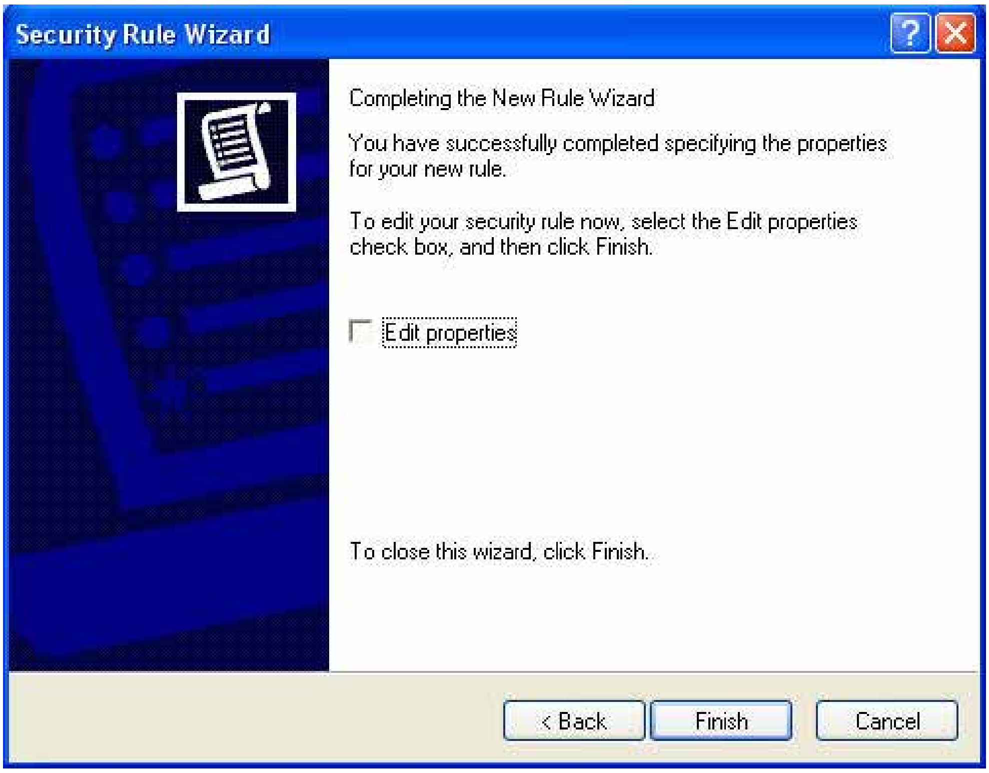
If no filter actions in the following list matches your needs, click Add to create a new one. Select Use Add Wizard to create a filter action using the wizard.

Filter Actions:

☑ Use Add Wizard

Name	Description
○ Permit	Permit unsecured IP packets t...
○ Request Security (Optional)	Accepts unsecured communi...
○ Require Security	Accepts unsecured communi...
● Security	

Step 36. Click finish.



Security Rule Wizard

Completing the New Rule Wizard

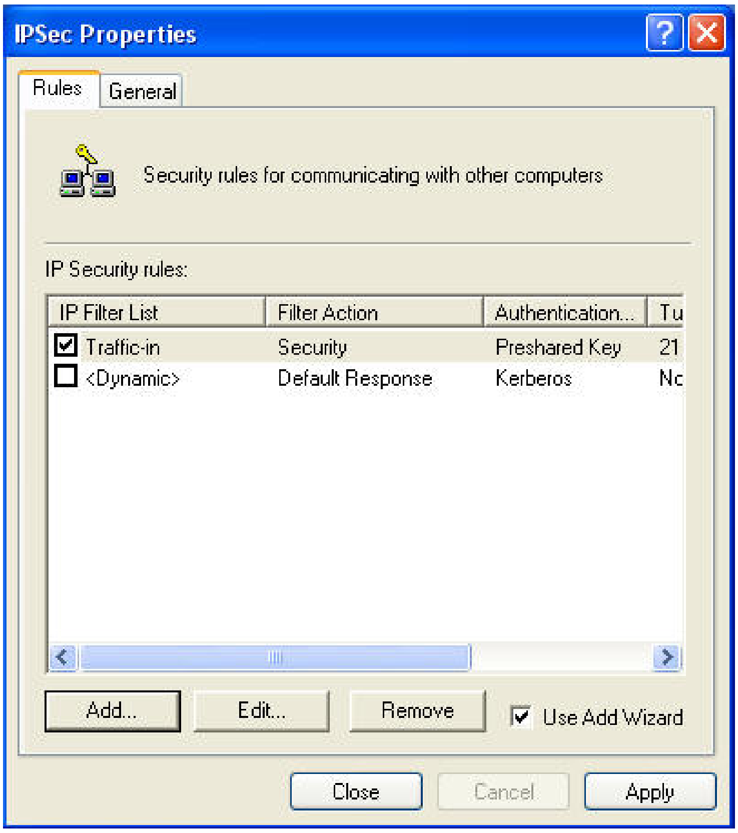
You have successfully completed specifying the properties for your new rule.

To edit your security rule now, select the Edit properties check box, and then click Finish.

□ Edit properties

To close this wizard, click Finish.

Step 37. Click Add.

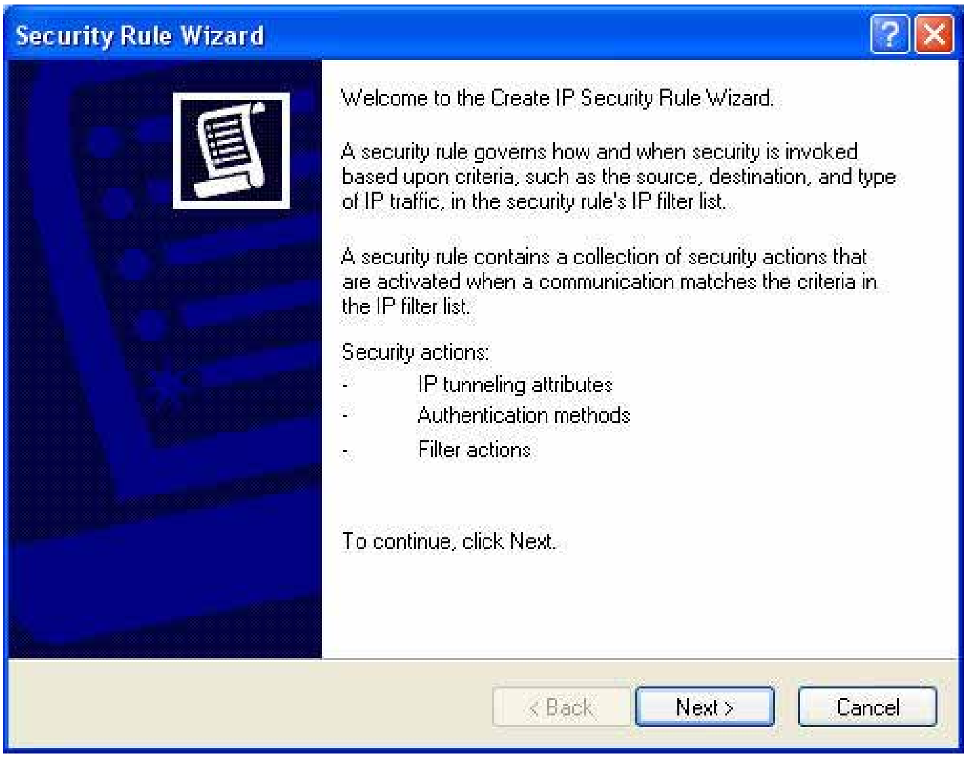


Security rules for communicating with other computers

IP Security rules:

IP Filter List	Filter Action	Authentication...	Tu
☑ Traffic-in	Security	Preshared Key	21
□ <Dynamic>	Default Response	Kerberos	Nc

Step 38. Click next.



Welcome to the Create IP Security Rule Wizard.

A security rule governs how and when security is invoked based upon criteria, such as the source, destination, and type of IP traffic, in the security rule's IP filter list.

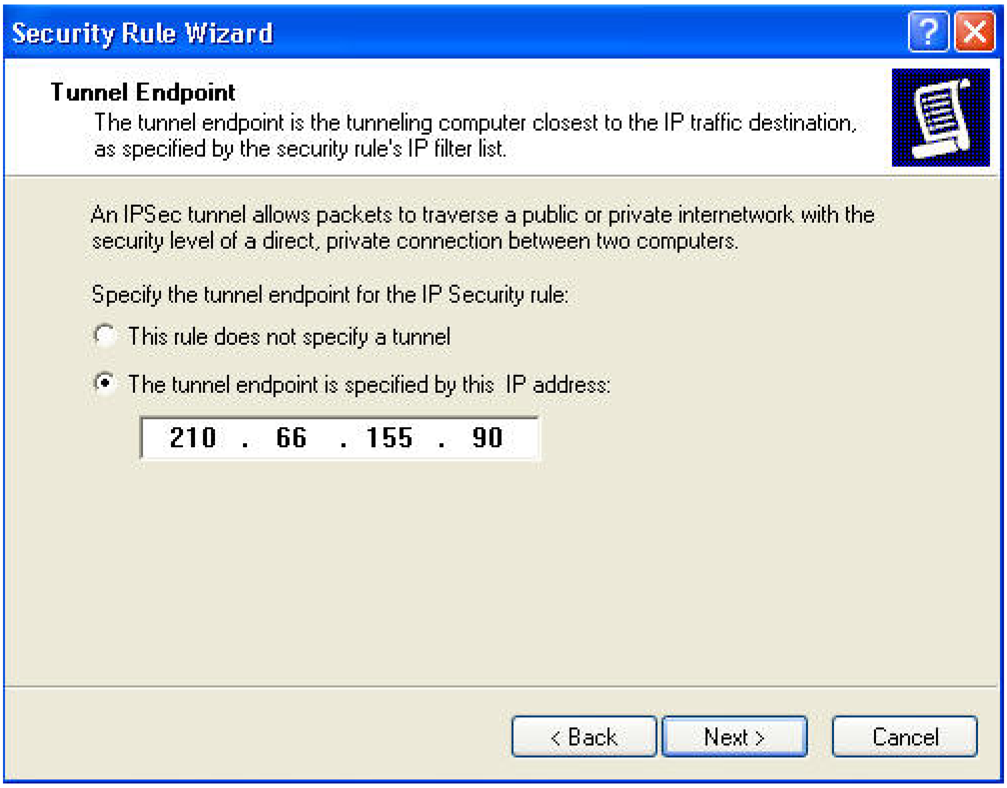
A security rule contains a collection of security actions that are activated when a communication matches the criteria in the IP filter list.

Security actions:

- IP tunneling attributes
- Authentication methods
- Filter actions

To continue, click Next.

Step 39. Enter the WAN IP of company A, 210.66.155.90.



Tunnel Endpoint

The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the security rule's IP filter list.

An IPSec tunnel allows packets to traverse a public or private internetwork with the security level of a direct, private connection between two computers.

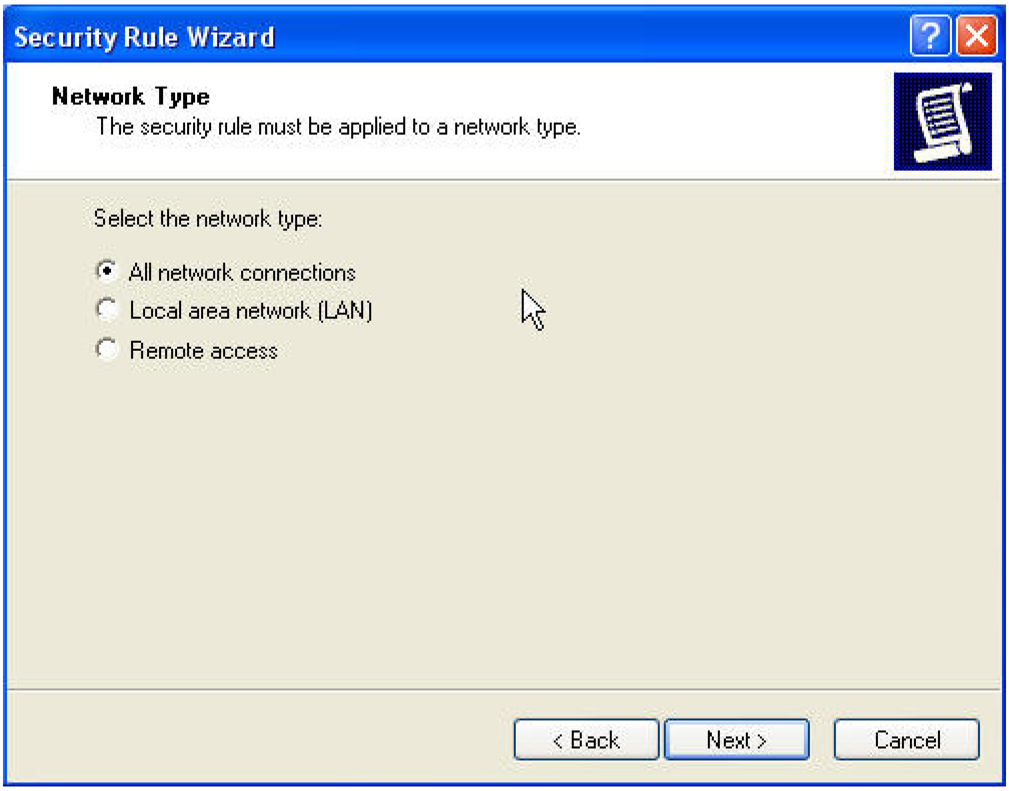
Specify the tunnel endpoint for the IP Security rule:

○ This rule does not specify a tunnel

● The tunnel endpoint is specified by this IP address:

210 . 66 . 155 . 90

Step 40. Select All network connections and click next.



Network Type

The security rule must be applied to a network type.

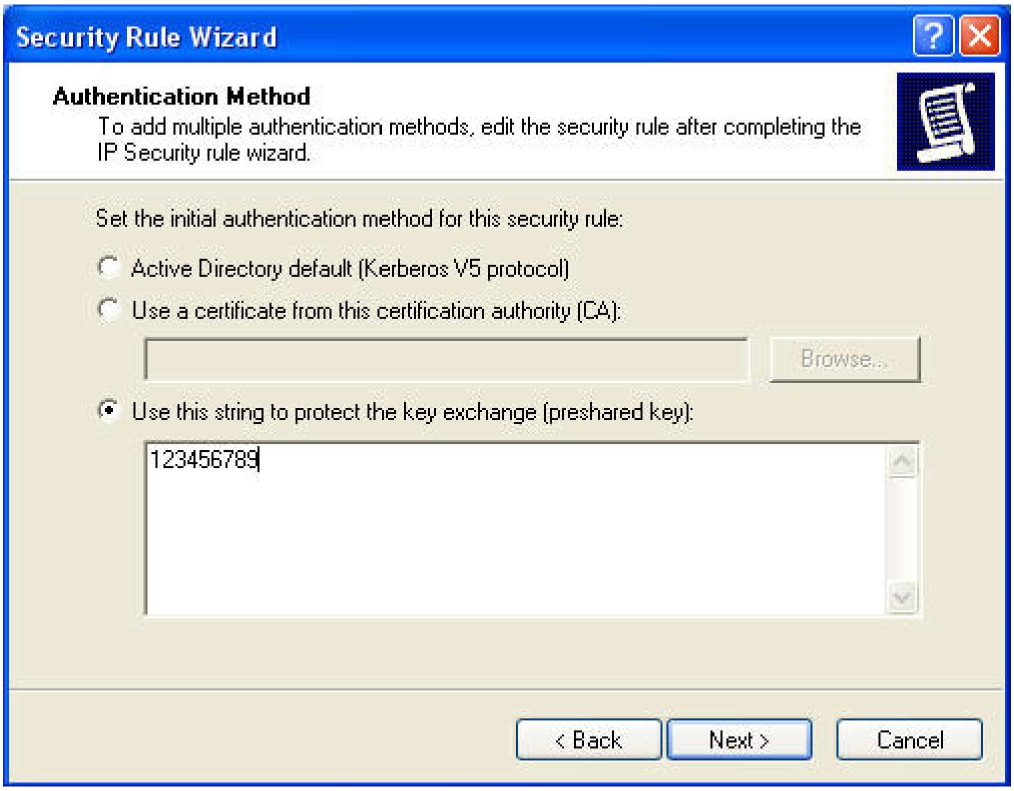
Select the network type:

● All network connections

○ Local area network (LAN)

○ Remote access

Step 41. Choose Use this string to protect the key exchange (Preshared Key). And enter the key, 123456789.



Security Rule Wizard

Authentication Method

To add multiple authentication methods, edit the security rule after completing the IP Security rule wizard.

Set the initial authentication method for this security rule:

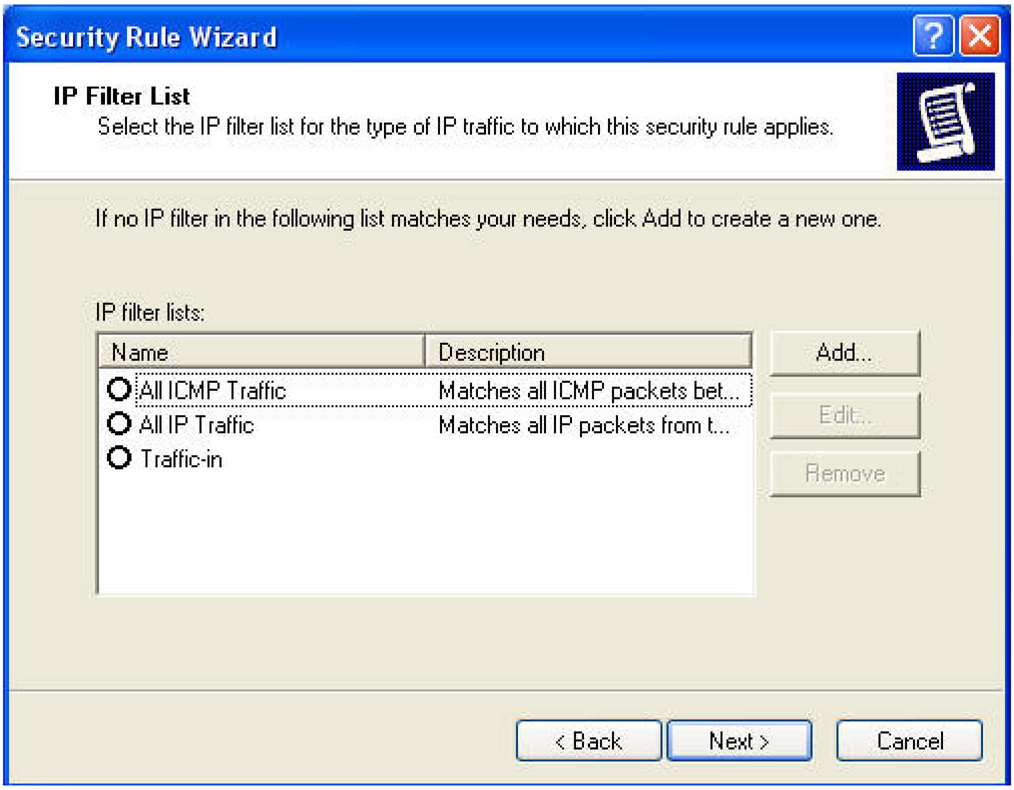
○ Active Directory default (Kerberos V5 protocol)

○ Use a certificate from this certification authority (CA):

● Use this string to protect the key exchange (preshared key):

123456789

Step 42. Click Add.



Security Rule Wizard

IP Filter List

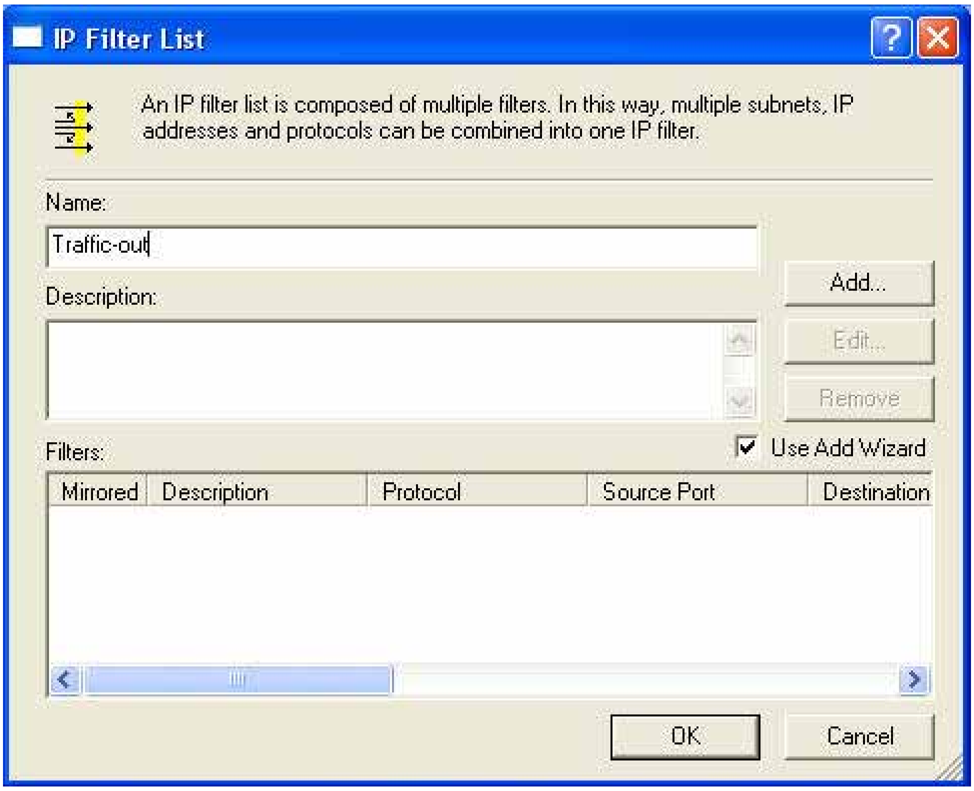
Select the IP filter list for the type of IP traffic to which this security rule applies.

If no IP filter in the following list matches your needs, click Add to create a new one.

IP filter lists:

Name	Description
○ All ICMP Traffic	Matches all ICMP packets bet...
○ All IP Traffic	Matches all IP packets from t...
○ Traffic-in	

Step 43. Enter the name of IP filter and click "Add…".



IP Filter List

An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter.

Name:

Traffic-out

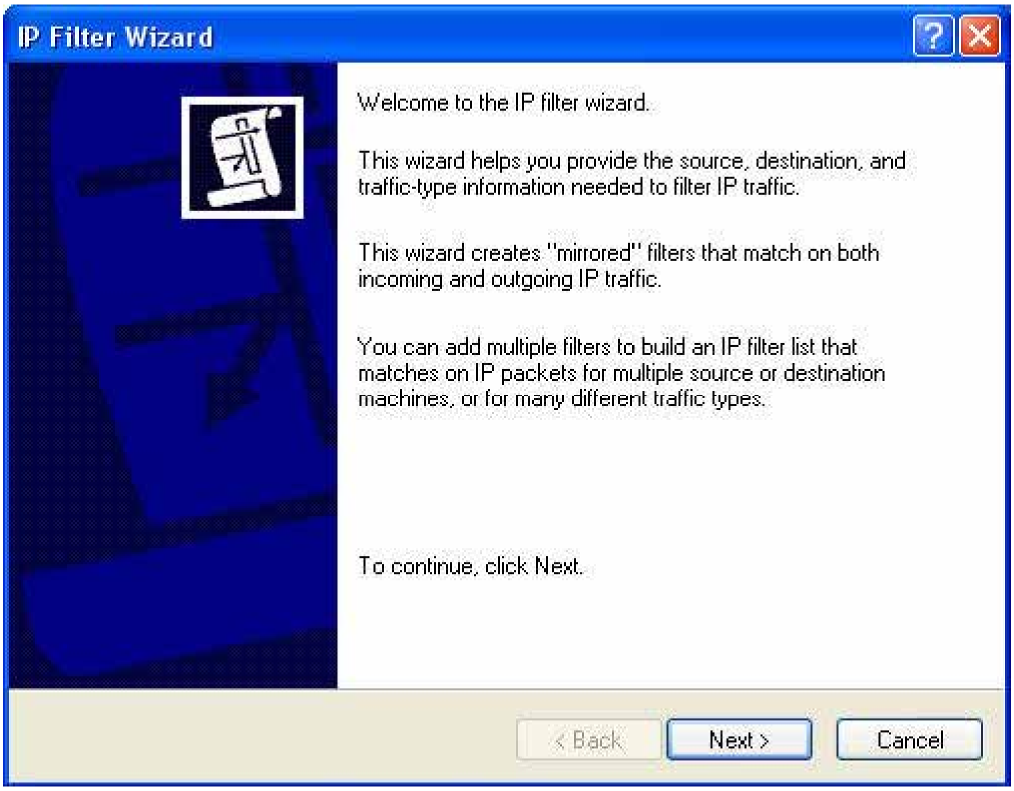
Description:

Filters:

☑ Use Add Wizard

Mirrored	Description	Protocol	Source Port	Destination

Step 44. Click next



IP Filter Wizard

Welcome to the IP filter wizard.

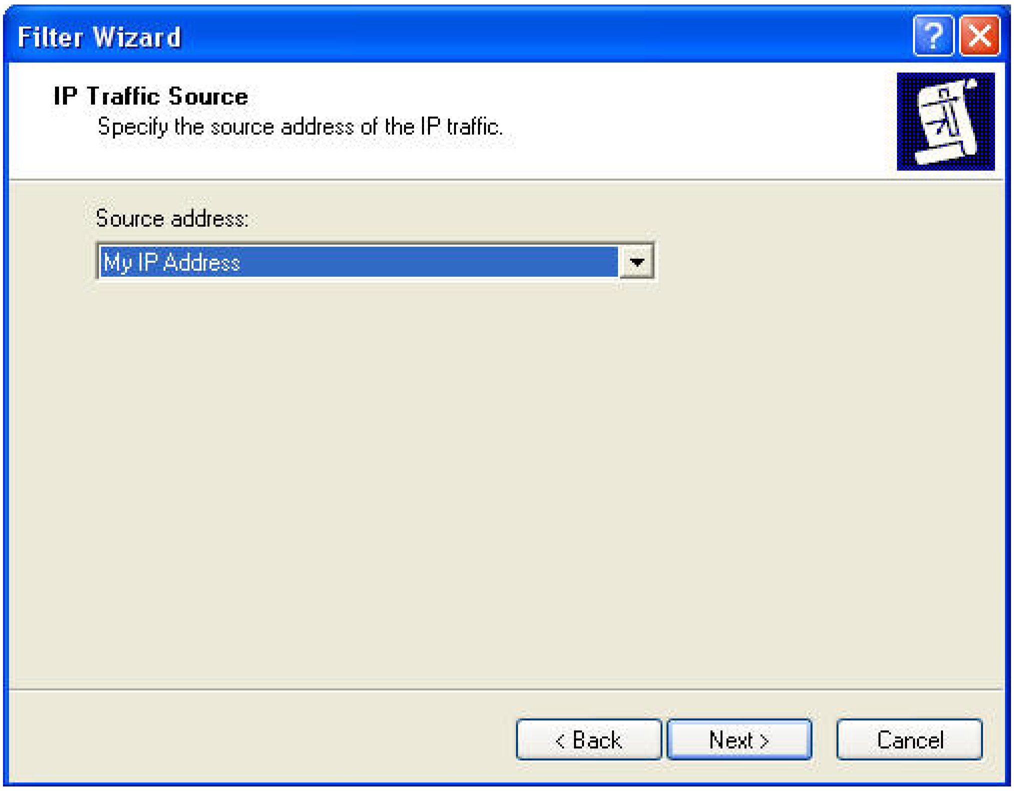
This wizard helps you provide the source, destination, and traffic-type information needed to filter IP traffic.

This wizard creates "mirrored" filters that match on both incoming and outgoing IP traffic.

You can add multiple filters to build an IP filter list that matches on IP packets for multiple source or destination machines, or for many different traffic types.

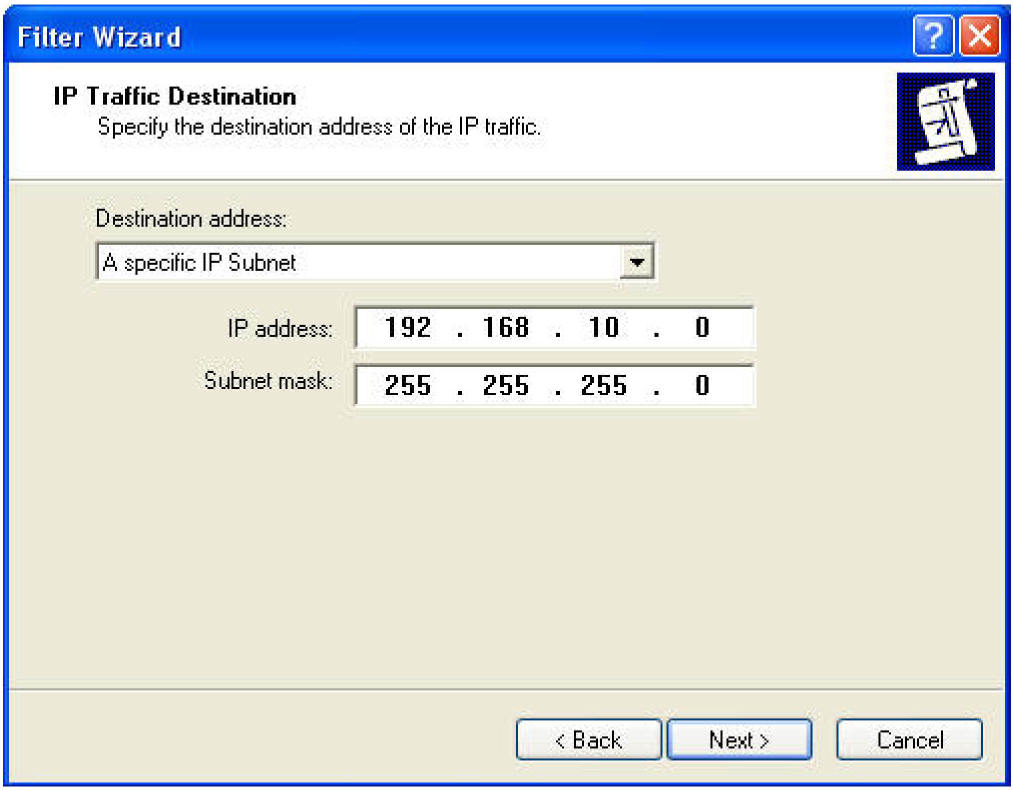
To continue, click Next.

Step 45. In Source address, click down the arrow to select the My IP Address.



Source address: My IP Address

Step 46. In Destination address, click down the arrow to select the specific IP Subnet and fill Company A's IP Address, 192.168.10.0 and Subnet mask 255.255.255.0.

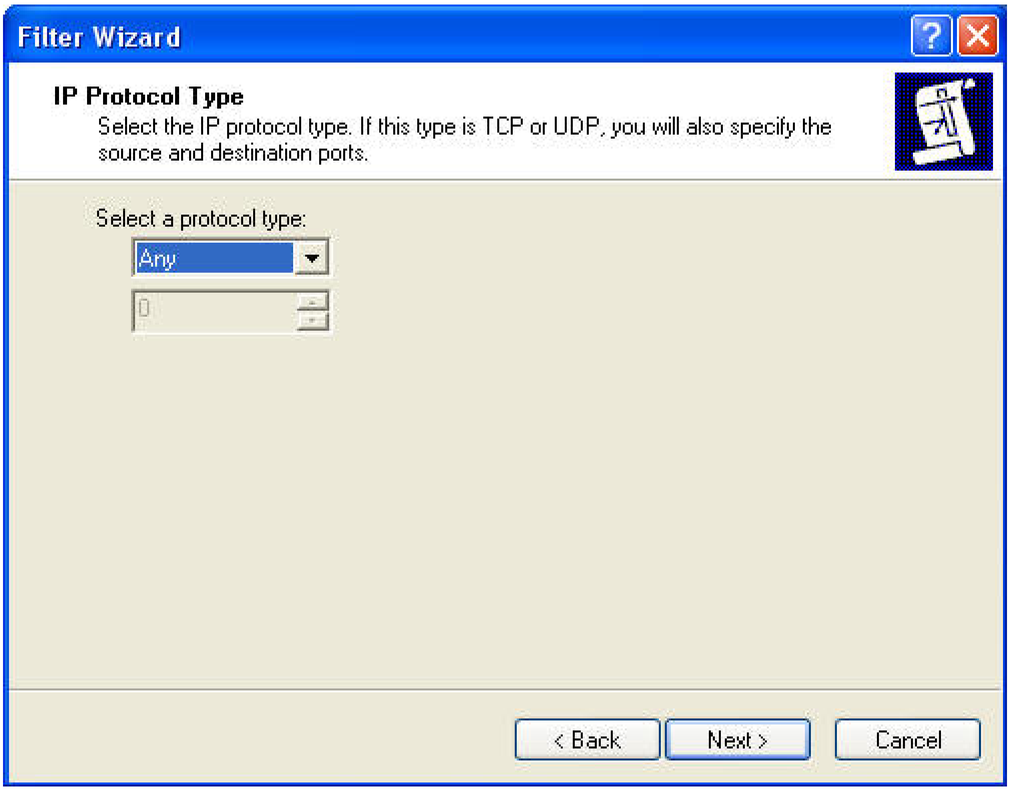


Destination address: A specific IP Subnet

IP address: 192 . 168 . 10 . 0

Subnet mask: 255 . 255 . 255 . 0

Step 47. Click next.



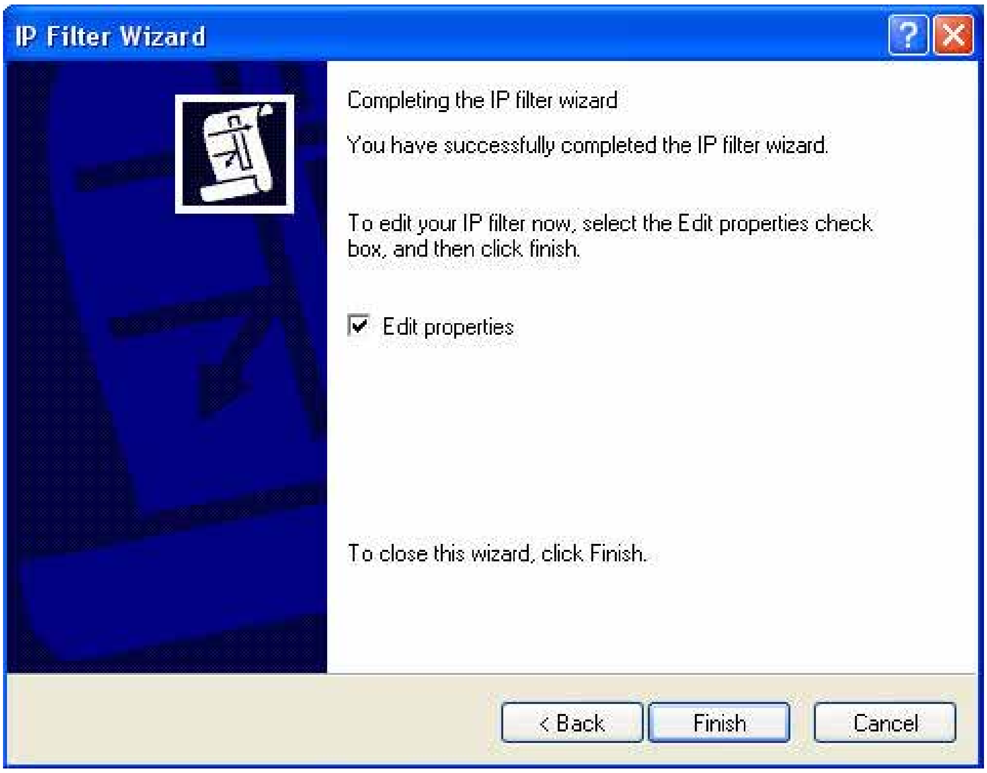
IP Protocol Type

Select the IP protocol type. If this type is TCP or UDP, you will also specify the source and destination ports.

Select a protocol type: Any

0

Step 48. Please enable Edit properties and click finish.



Completing the IP filter wizard

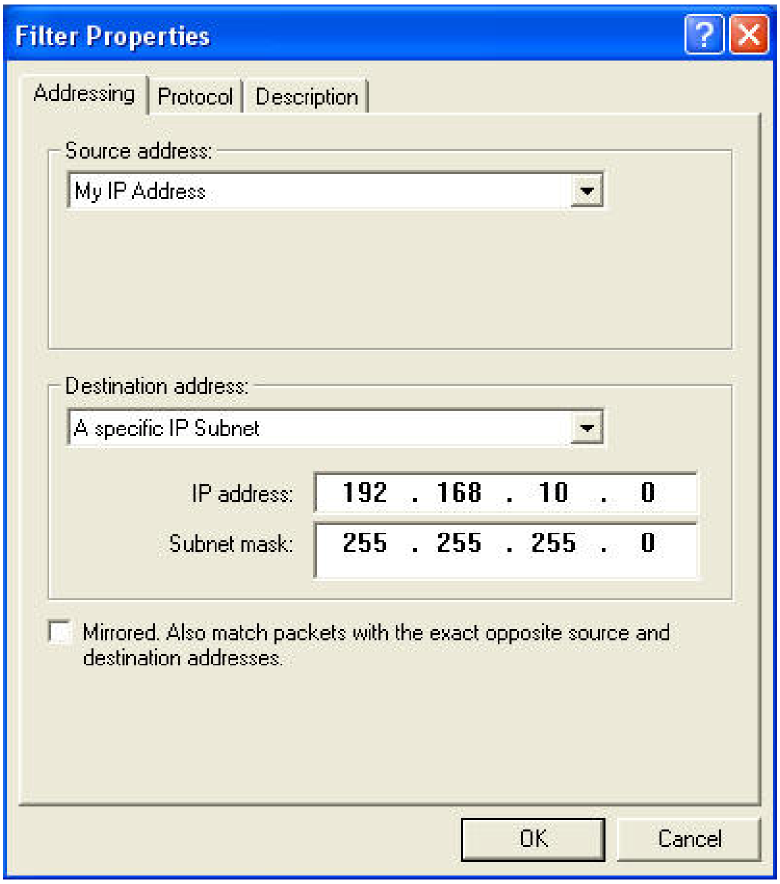
You have successfully completed the IP filter wizard.

To edit your IP filter now, select the Edit properties check box, and then click finish.

☑ Edit properties

To close this wizard, click Finish.

Step 49. Please don't enable Mirrored and click ok.



Source address:
My IP Address

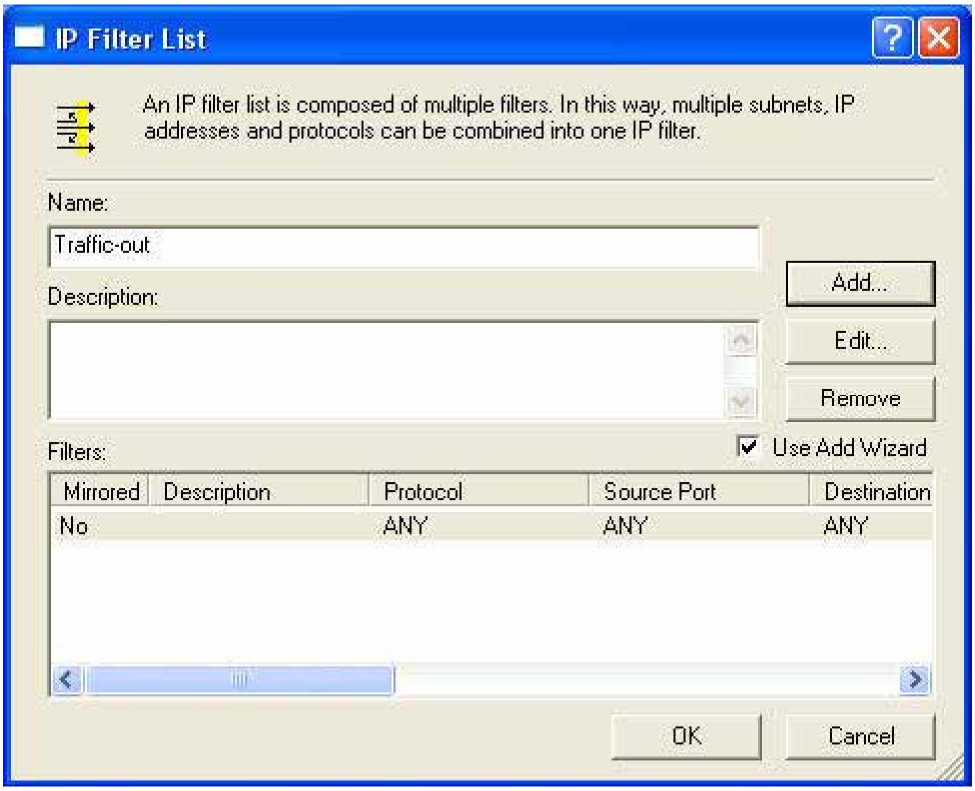
Destination address:
A specific IP Subnet

IP address: 192 . 168 . 10 . 0

Subnet mask: 255 . 255 . 255 . 0

□ Mirrored. Also match packets with the exact opposite source and destination addresses.

Step 50. Click ok.



An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter.

Name:
Traffic-out

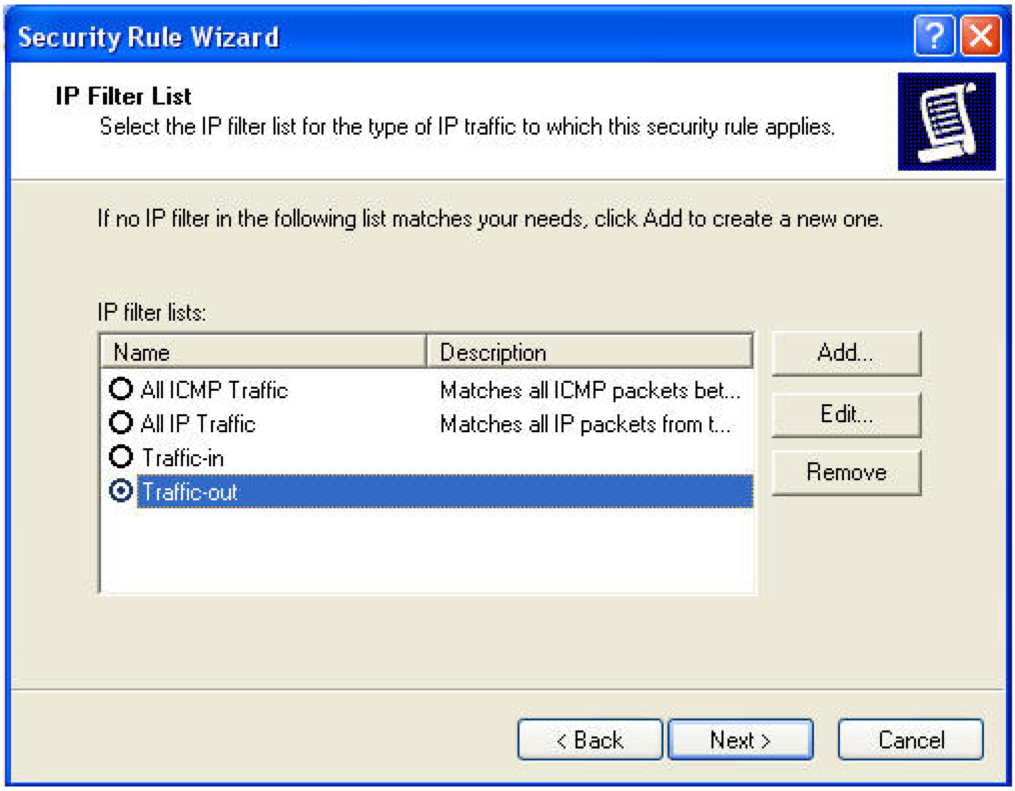
Description:

Filters:

☑ Use Add Wizard

Mirrored	Description	Protocol	Source Port	Destination
No		ANY	ANY	ANY

Step 51. Select Traffic-out and click next.



IP Filter List

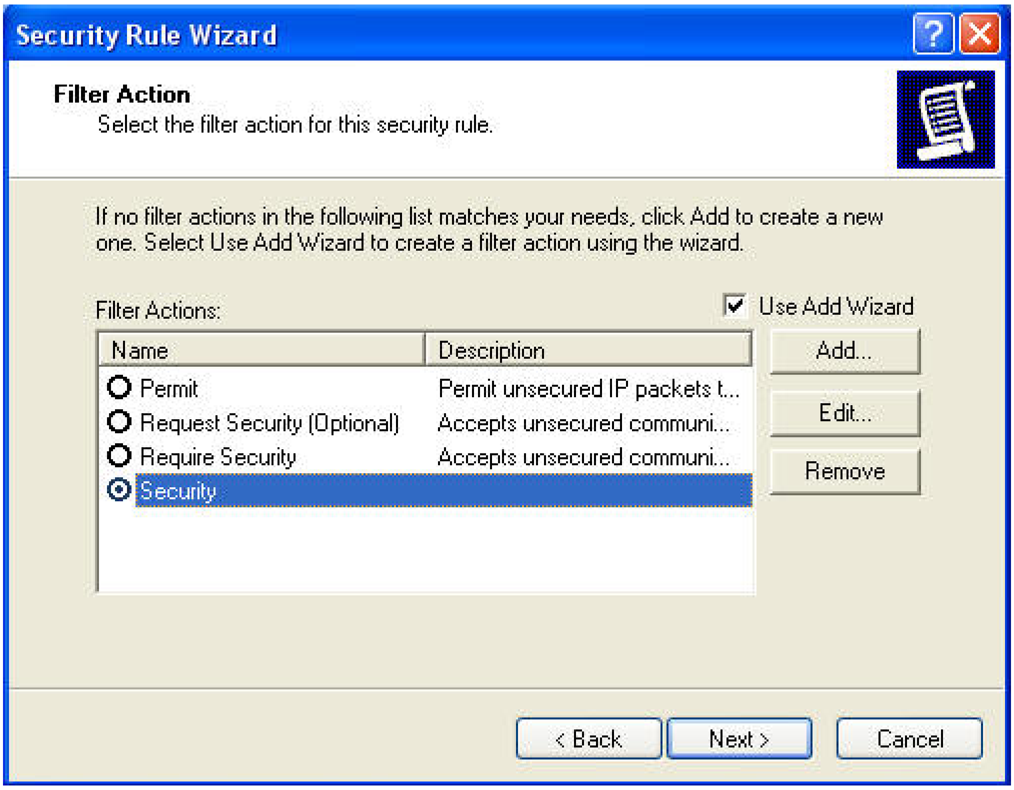
Select the IP filter list for the type of IP traffic to which this security rule applies.

If no IP filter in the following list matches your needs, click Add to create a new one.

IP filter lists:

Name	Description
○ All ICMP Traffic	Matches all ICMP packets bet...
○ All IP Traffic	Matches all IP packets from t...
○ Traffic-in	
● Traffic-out	

Step 52. Select Security and click edit.



Filter Action

Select the filter action for this security rule.

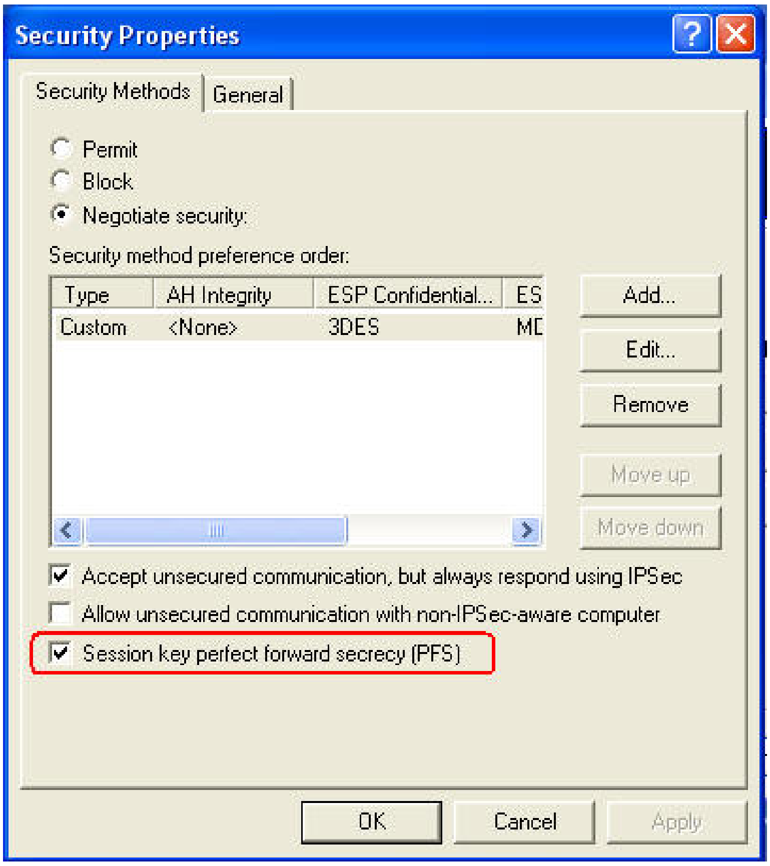
If no filter actions in the following list matches your needs, click Add to create a new one. Select Use Add Wizard to create a filter action using the wizard.

Filter Actions:

☑ Use Add Wizard

Name	Description
○ Permit	Permit unsecured IP packets t...
○ Request Security (Optional)	Accepts unsecured communi...
○ Require Security	Accepts unsecured communi...
● Security	

Step 53. Enable Session key perfect forward secrecy (PFS) and click ok.



Security Properties

Security Methods | General

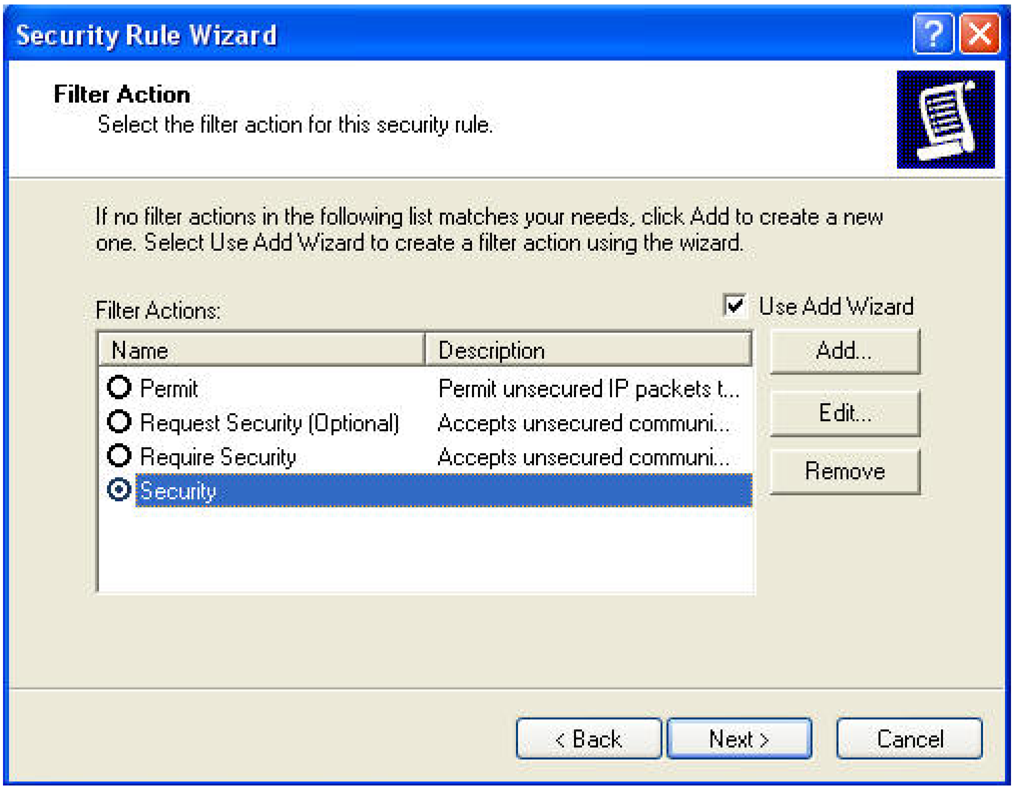
○ Permit
○ Block
● Negotiate security:

Security method preference order:

Type	AH Integrity	ESP Confidential...	ES
Custom	<None>	3DES	MD

☑ Accept unsecured communication, but always respond using IPSec
☐ Allow unsecured communication with non-IPSec-aware computer
☑ Session key perfect forward secrecy (PFS)

Step 54. Select Security and click next.



Security Rule Wizard

Filter Action
Select the filter action for this security rule.

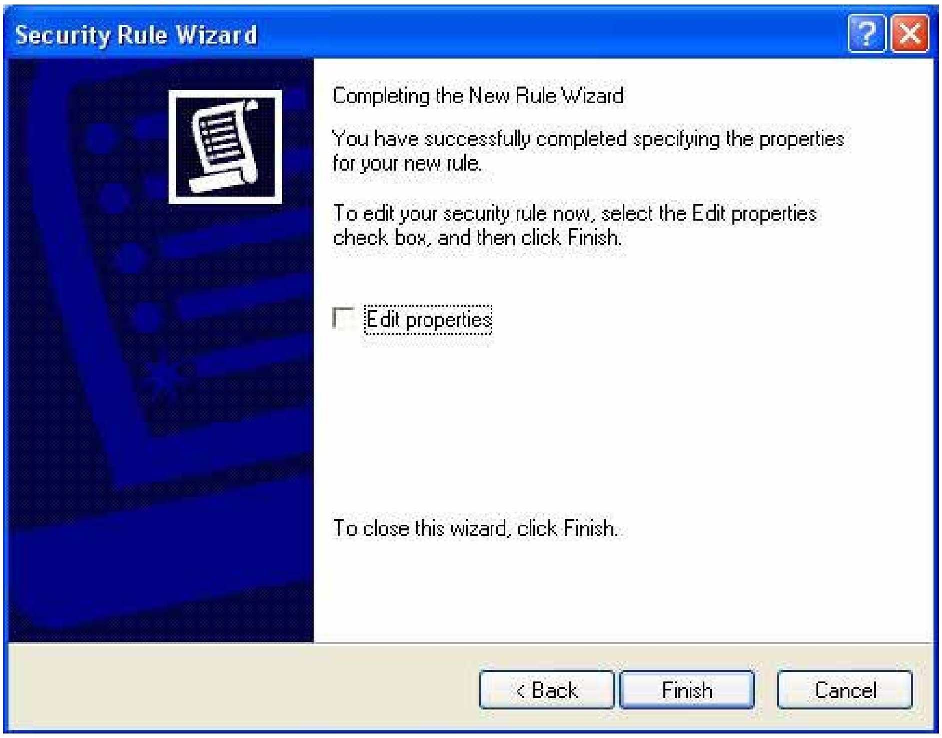
If no filter actions in the following list matches your needs, click Add to create a new one. Select Use Add Wizard to create a filter action using the wizard.

Filter Actions:

☑ Use Add Wizard

Name	Description
○ Permit	Permit unsecured IP packets t...
○ Request Security (Optional)	Accepts unsecured communi...
○ Require Security	Accepts unsecured communi...
● Security	

Step 55. Please don't enable Edit properties and click finish.



Security Rule Wizard

Completing the New Rule Wizard

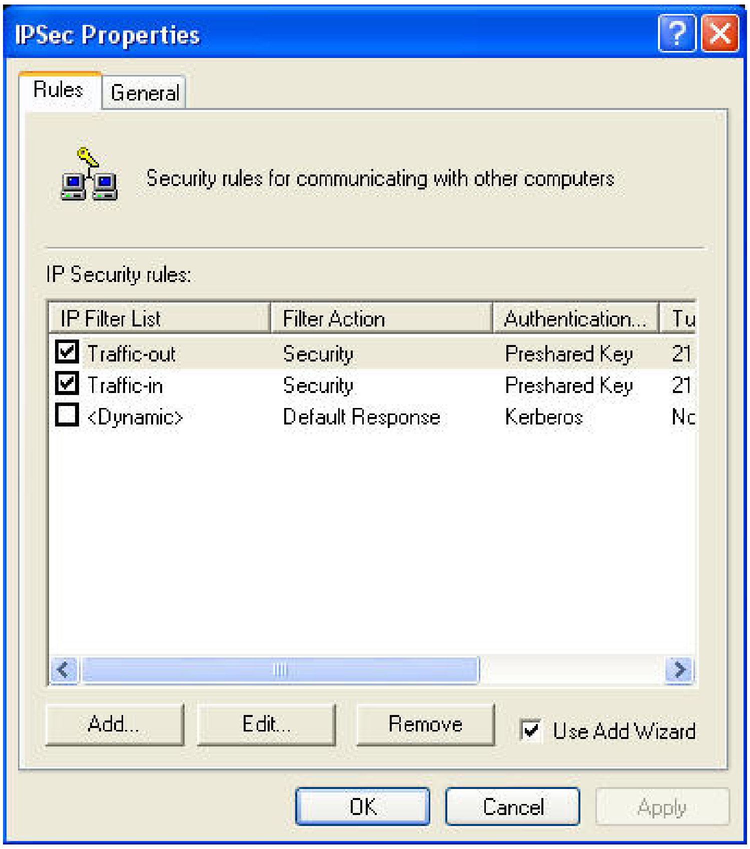
You have successfully completed specifying the properties for your new rule.

To edit your security rule now, select the Edit properties check box, and then click Finish.

☐ Edit properties

To close this wizard, click Finish.

Step 56. Click apply first and then click ok.



IPSec Properties

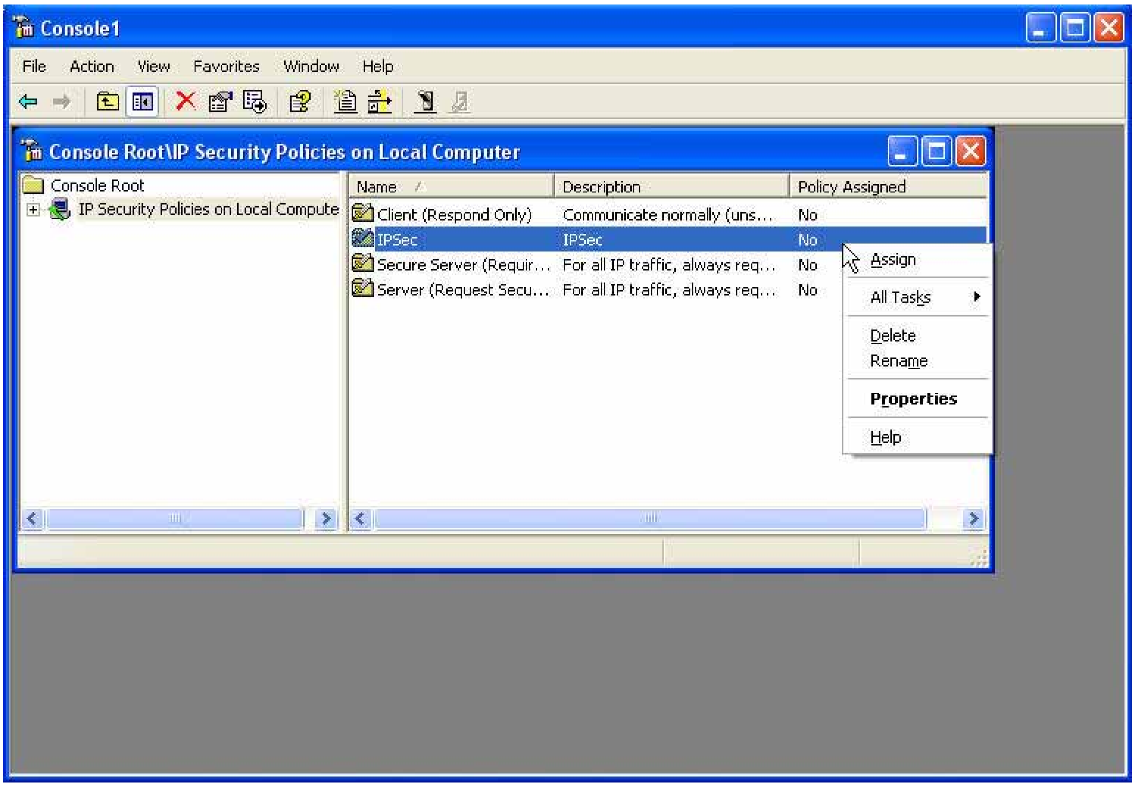
Security rules for communicating with other computers

IP Security rules:

IP Filter List	Filter Action	Authentication...	Tu
☑ Traffic-out	Security	Preshared Key	21
☑ Traffic-in	Security	Preshared Key	21
☐ <Dynamic>	Default Response	Kerberos	Nc

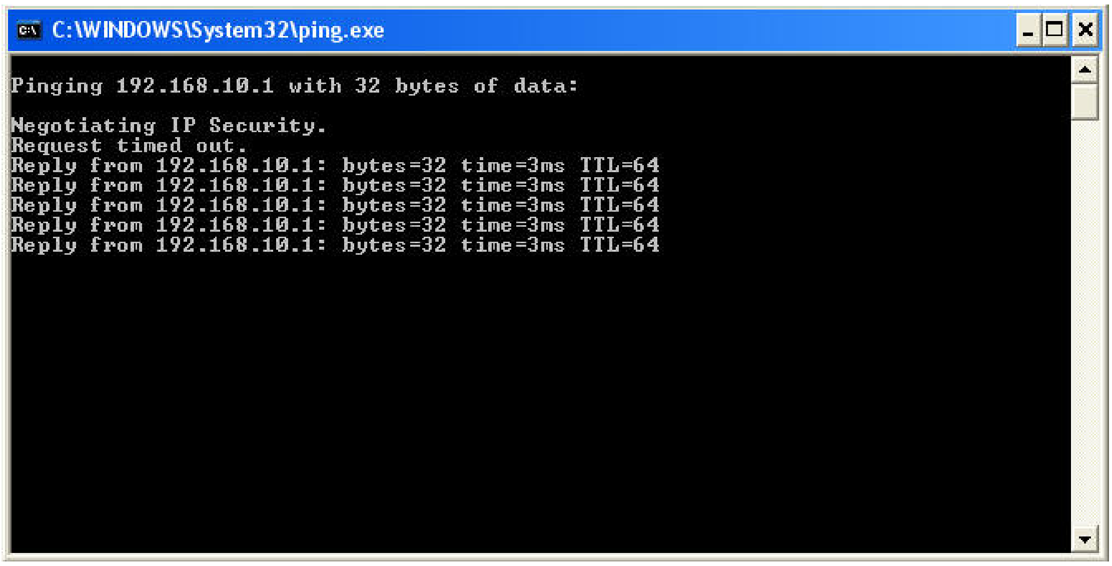
☑ Use Add Wizard

Step 57 Click the right button of mouse in IPSec choose Assign option.


Console1
File Action View Favorites Window Help
Console Root\IP Security Policies on Local Computer
Console Root
IP Security Policies on Local Compute
Assign
All Tasks
Delete
Rename
Properties
Help

Name	Description	Policy Assigned
Client (Respond Only)	Communicate normally (uns...	No
IPSec	IPSec	No
Secure Server (Requir...	For all IP traffic, always req...	No
Server (Request Secu...	For all IP traffic, always req...	No

Step 58. Ping the remote gateway of Company A, the VPN tunnel is created successfully.


C:\WINDOWS\System32\ping.exe

```
Pinging 192.168.10.1 with 32 bytes of data:

Negotiating IP Security.
Request timed out.
Reply from 192.168.10.1: bytes=32 time=3ms TTL=64
Reply from 192.168.10.1: bytes=32 time=3ms TTL=64
Reply from 192.168.10.1: bytes=32 time=3ms TTL=64
Reply from 192.168.10.1: bytes=32 time=3ms TTL=64
Reply from 192.168.10.1: bytes=32 time=3ms TTL=64
```

Example 3. Create a VPN connection between two Content Security Gateways using Aggressive mode Algorithm (3 DES and MD5), and data encryption for IPSec Algorithm (3DES and MD5)

Preparation Task:

Company A External IP is 61.11.11.11

Internal IP is 192.168.10.X

Company B External IP is 211.22.22.22

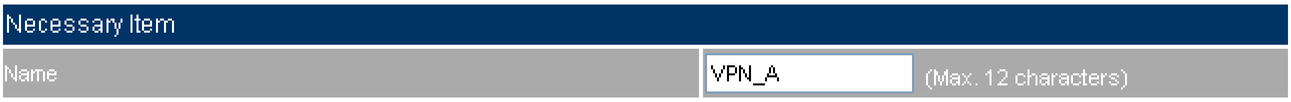
Internal IP is 192.168.20.X

To Allow Company A, 192.168.10.100 create a VPN connection with company B, 192.168.20.100 for downloading the sharing file.

The Gateway of Company A is 192.168.10.1. The settings of company A are as the following.

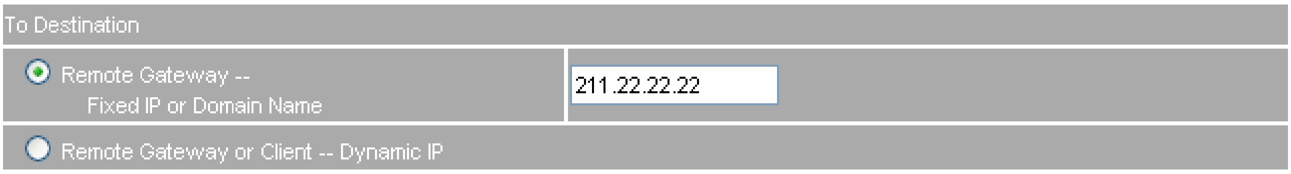
Step 1. Enter the default IP of Company A's Content Security Gateway, 192.168.10.1. Click VPN in the menu bar on the left hand side, and then select the sub-select IPSec Autokey. Click Add.

Step 2. Enter the VPN name, VPN_A in IPSec Autokey window.



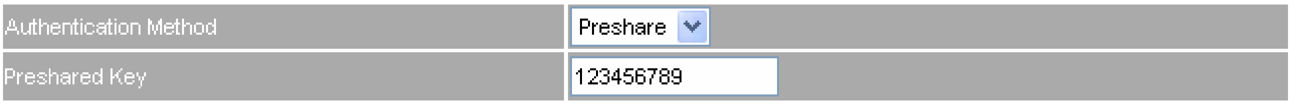
Necessary Item	
Name	VPN_A (Max. 12 characters)

Step 3. In To Destination table, choose Remote Gateway-Fixed IP or Domain Name, enter the IP address desired to be connected.



To Destination	
● Remote Gateway -- Fixed IP or Domain Name	211.22.22.22
○ Remote Gateway or Client -- Dynamic IP	

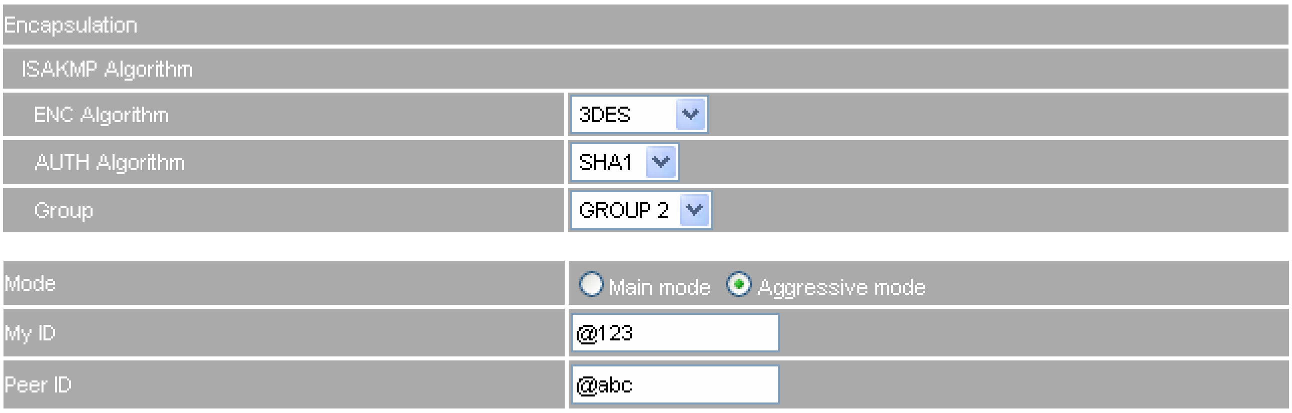
Step 4. In Authentication Method Table enters the Preshared Key.



Authentication Method	Preshare
Preshared Key	123456789

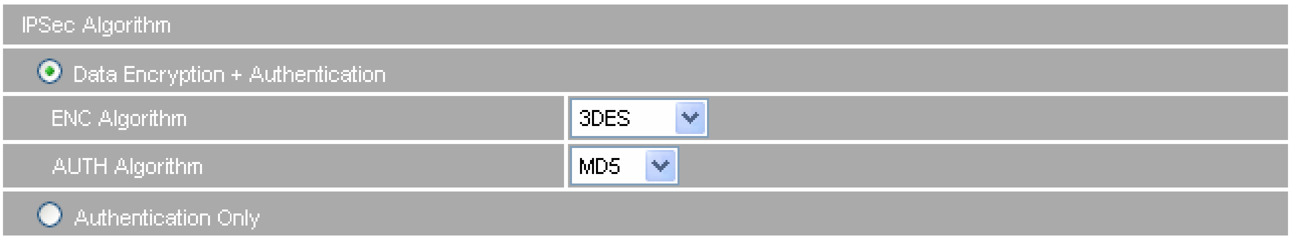
Step 5. Enable Aggressive mode. For communication via VPN, the Content Security Gateway will force you to choose 3DES for ENC Algorithm, SHA-1 for AUTH Algorithm and select Group 2 to connect.

Local ID and Remote ID are optional parameters. If we choose to enter Local ID/ Remote ID, they couldn't be the same. For instance, Local ID is 11.11.11.11 and Remote ID is 22.22.22.22. If you want to use number or text, add @ in the front, for instance, @123 and @abc.



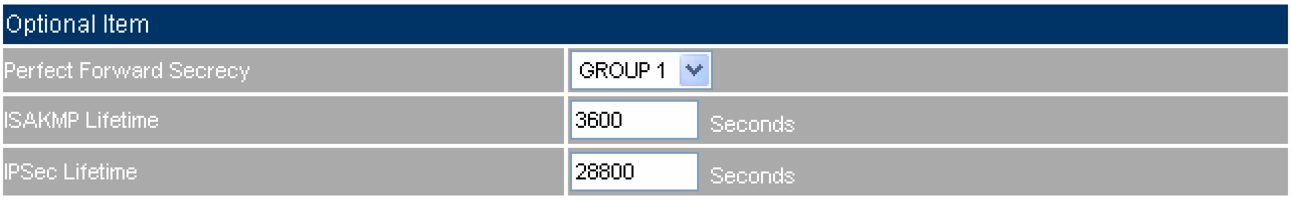
Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	3DES
AUTH Algorithm	SHA1
Group	GROUP 2
Mode	○ Main mode ● Aggressive mode
My ID	@123
Peer ID	@abc

Step 6. In IPSec Algorithm Table, choose Data Encryption + Authentication. We choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm.



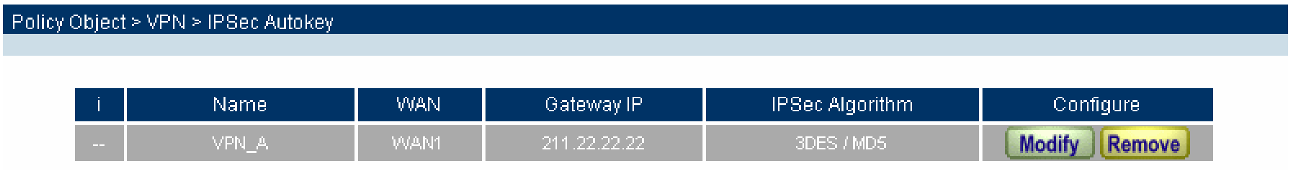
IPSec Algorithm	
● Data Encryption + Authentication	
ENC Algorithm	3DES
AUTH Algorithm	MD5
○ Authentication Only	

Step 7. Choose GROUP 1 as the Perfect Forward Secrecy setting, and leave the default setting with 28800 seconds in IPSec Lifetime and 3600 seconds for ISAKMP Lifetime.



Optional Item	
Perfect Forward Secrecy	GROUP 1
ISAKMP Lifetime	3600 Seconds
IPSec Lifetime	28800 Seconds

Step 8. Click OK to finish the setting of Company A.

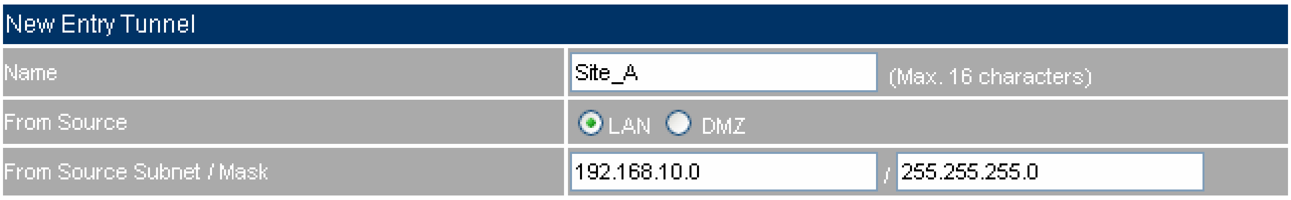


Policy Object > VPN > IPSec Autokey

i	Name	WAN	Gateway IP	IPSec Algorithm	Configure
--	VPN_A	WAN1	211.22.22.22	3DES / MD5	Modify Remove

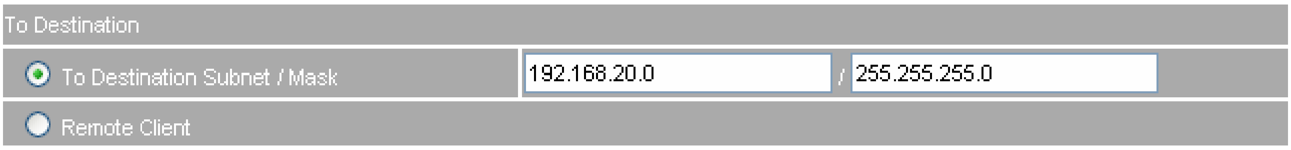
Step 9. Click Tunnel and press New Entry to configure the further setting.

Step 10. Enter Site_A as the new tunnel name, and select LAN interface as the VPN source. Fill LAN IP subnet 192.168.10.0 with subnet mask IP 255.255.255.0.



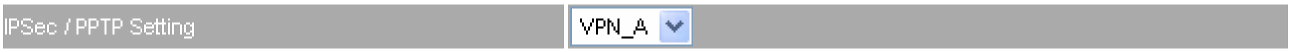
New Entry Tunnel	
Name	Site_A (Max. 16 characters)
From Source	● LAN ○ DMZ
From Source Subnet / Mask	192.168.10.0 / 255.255.255.0

Step 11. In To Destination table, fill company B's subnet IP and mask, 192.168.20.0 and 255.255.255.0 respectively.



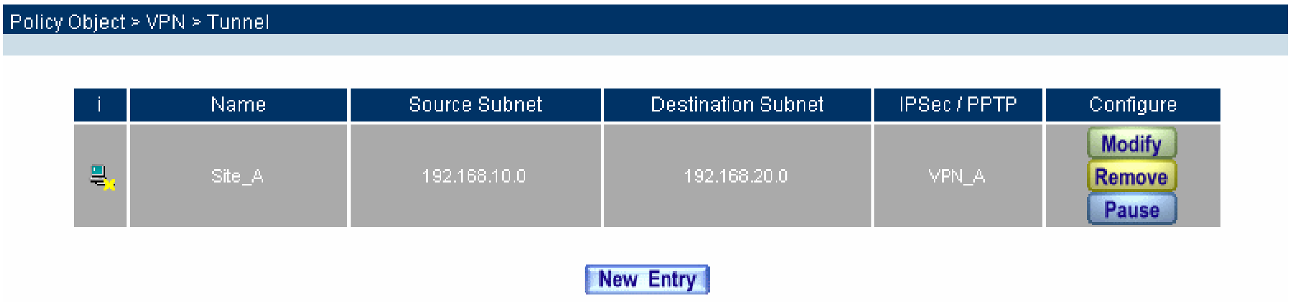
To Destination	
● To Destination Subnet / Mask	192.168.20.0 / 255.255.255.0
○ Remote Client	

Step 12. In IPSec / PPTP Setting, select VPN_A as the available tunnel.



IPSec / PPTP Setting	VPN_A

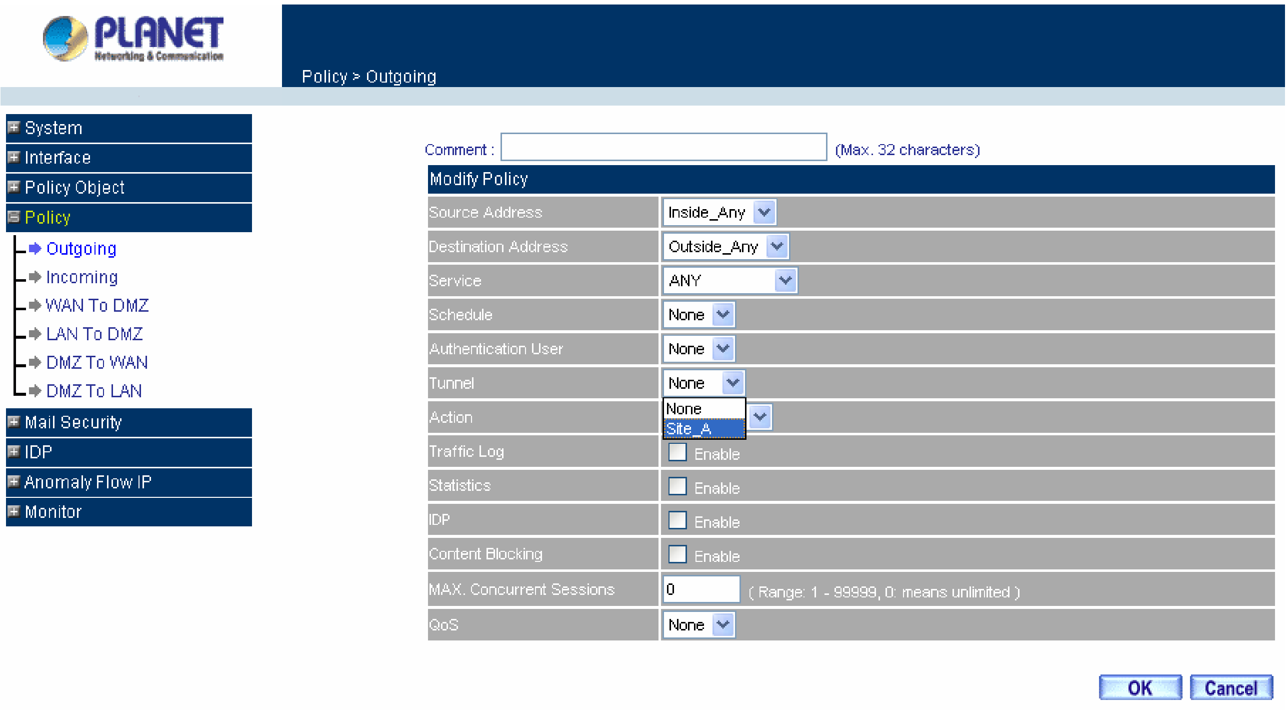
Step 13. Click OK to finish the Tunnel setting of Company A.



Policy Object > VPN > Tunnel

i	Name	Source Subnet	Destination Subnet	IPSec / PPTP	Configure
	Site_A	192.168.10.0	192.168.20.0	VPN_A	Modify Remove Pause

Step 14. If you want to configure bi-direction VPN connection, you should enable Tunnel setting in Outgoing and Incoming Policy.

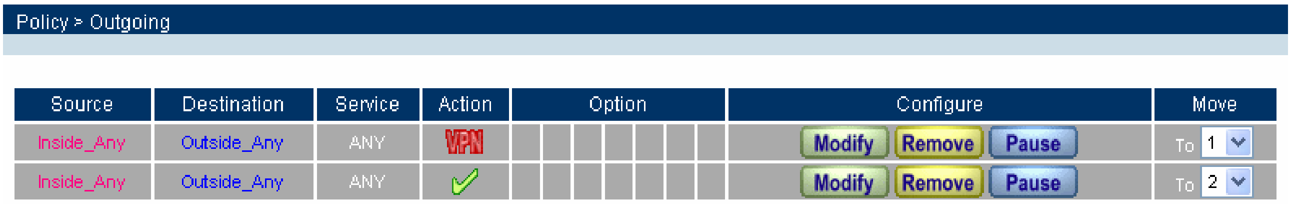


Policy > Outgoing

Comment : (Max. 32 characters)

Modify Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
Tunnel	None None Site_A
Action	
Traffic Log	□ Enable
Statistics	□ Enable
IDP	□ Enable
Content Blocking	□ Enable
MAX. Concurrent Sessions	0 (Range: 1 - 99999, 0: means unlimited)
QoS	None

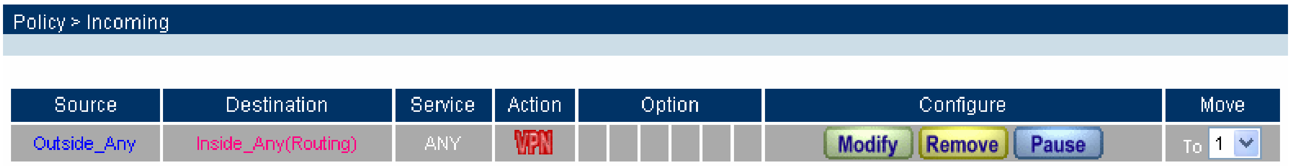
Outgoing Policy:



Policy > Outgoing

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	VPN		Modify Remove Pause	To 1
Inside_Any	Outside_Any	ANY	✓		Modify Remove Pause	To 2

Incoming Policy:



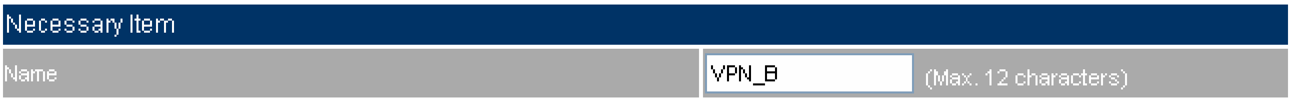
Policy > Incoming

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Inside_Any(Routing)	ANY	VPN		Modify Remove Pause	To 1

The Gateway of Company B is 192.168.20.1. The settings of company B are as the following.

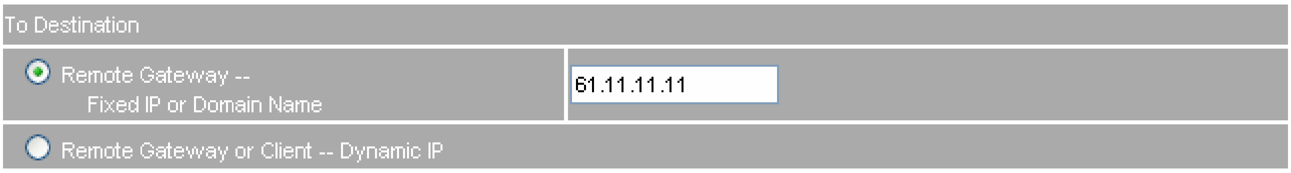
Step 1. Enter the default IP of Company B's Content Security Gateway, 192.168.20.1. Click VPN in the menu bar on the left hand side, and then select the sub-select IPSec Autokey. Click Add.

Step 2. Enter the VPN name, VPN_B in IPSec Autokey window.



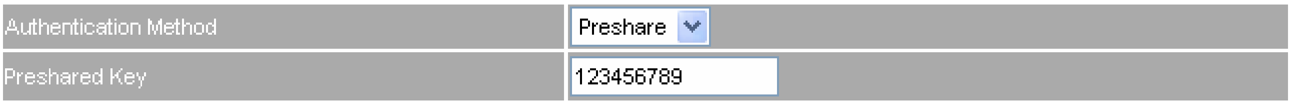
Necessary Item	
Name	VPN_B (Max. 12 characters)

Step 3. In To Destination table, choose Remote Gateway-Fixed IP or Domain Name, enter the IP address desired to be connected.



To Destination	
● Remote Gateway -- Fixed IP or Domain Name	61.11.11.11
○ Remote Gateway or Client -- Dynamic IP	

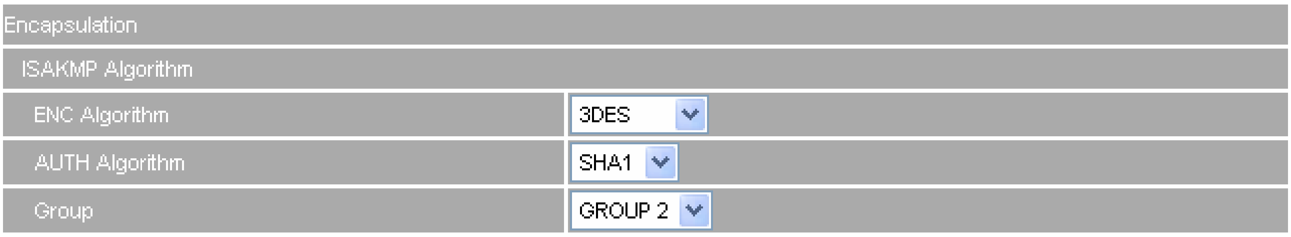
Step 4. In Authentication Method Table enters the Preshared Key.



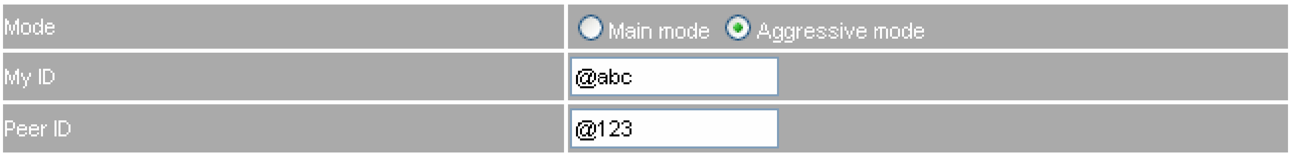
Authentication Method	Preshare
Preshared Key	123456789

Step 5. Enable Aggressive mode. For communication via VPN, the Content Security Gateway will force you to choose 3DES for ENC Algorithm, SHA-1 for AUTH Algorithm and select Group 2 to connect.

Local ID and Remote ID are optional parameters. If we choose to enter Local ID/ Remote ID, they couldn't be the same. For instance, Local ID is 11.11.11.11 and Remote ID is 22.22.22.22. If you want to use number or text, add @ in the front, for instance, @123 and @abc.

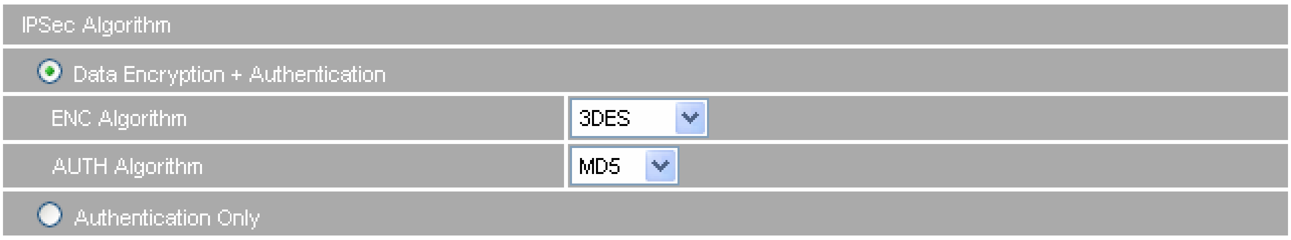


Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	3DES
AUTH Algorithm	SHA1
Group	GROUP 2



Mode	○ Main mode ● Aggressive mode
My ID	@abc
Peer ID	@123

Step 6. In IPSec Algorithm Table, choose Data Encryption + Authentication. We choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm.



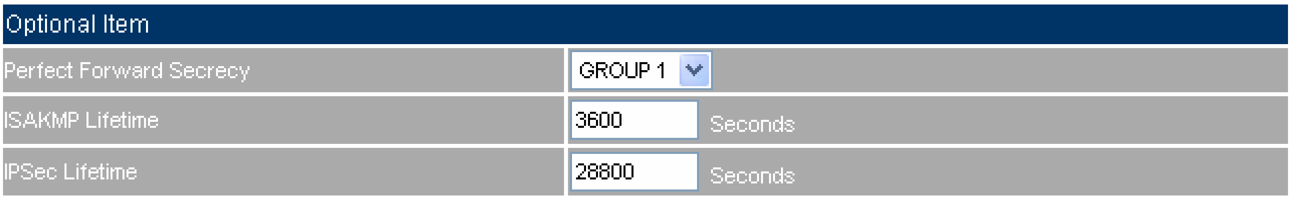
IPSec Algorithm

● Data Encryption + Authentication

ENC Algorithm	3DES
AUTH Algorithm	MD5

○ Authentication Only

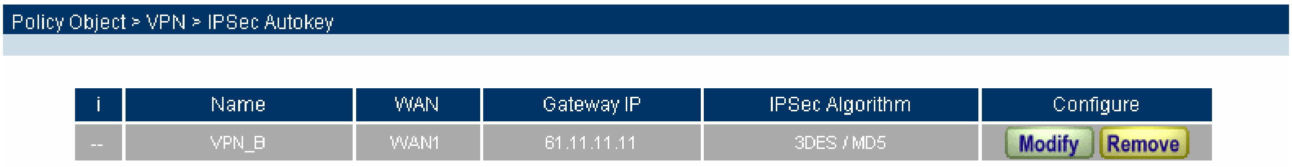
Step 7. Choose GROUP 1 as the Perfect Forward Secrecy setting, and leave the default setting with 28800 seconds in IPSec Lifetime and 3600 seconds for ISAKMP Lifetime.



Optional Item

Perfect Forward Secrecy	GROUP 1
ISAKMP Lifetime	3600 Seconds
IPSec Lifetime	28800 Seconds

Step 8. Click OK to finish the setting of Company B.

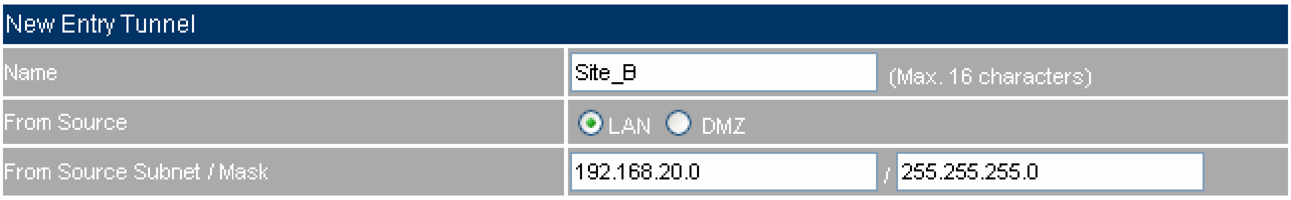


Policy Object > VPN > IPSec Autokey

i	Name	WAN	Gateway IP	IPSec Algorithm	Configure
--	VPN_B	WAN1	61.11.11.11	3DES / MD5	Modify Remove

Step 9. Click Tunnel and press New Entry to configure the further setting.

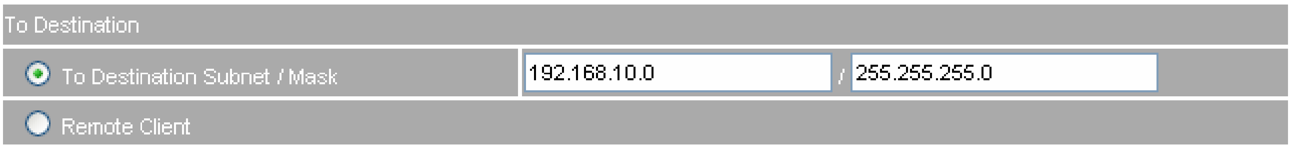
Step 10. Enter Site_B as the new tunnel name, and select LAN interface as the VPN source. Fill LAN IP subnet 192.168.20.0 with subnet mask IP 255.255.255.0.



New Entry Tunnel

Name	Site_B (Max. 16 characters)
From Source	● LAN ○ DMZ
From Source Subnet / Mask	192.168.20.0 / 255.255.255.0

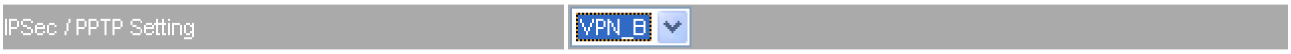
Step 11. In To Destination table, fill company A's subnet IP and mask, 192.168.10.0 and 255.255.255.0 respectively.



To Destination

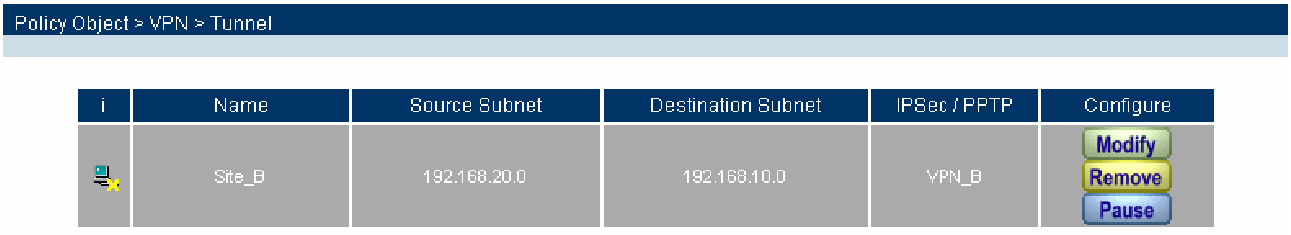
● To Destination Subnet / Mask	192.168.10.0 / 255.255.255.0
○ Remote Client	

Step 12. In IPSec /PPTP Setting, select VPN_B tunnel as the available tunnel.



IPSec / PPTP Setting	VPN_B

Step 13. Click OK to finish the Tunnel setting of Company B.

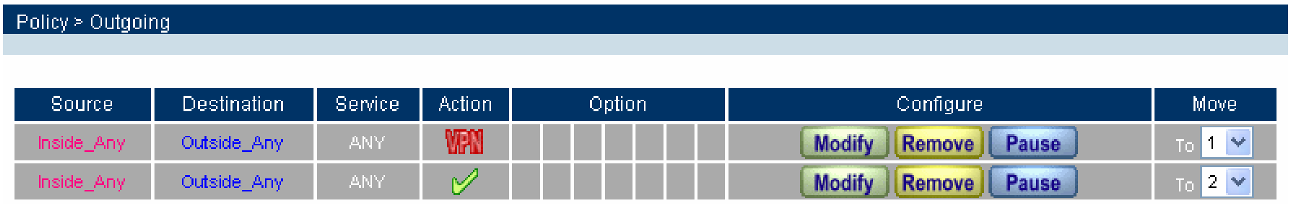


Policy Object > VPN > Tunnel

i	Name	Source Subnet	Destination Subnet	IPSec / PPTP	Configure
	Site_B	192.168.20.0	192.168.10.0	VPN_B	Modify Remove Pause

Step 14. If you want to configure bi-direction VPN connection, you should enable Tunnel setting in Outgoing and Incoming Policy.

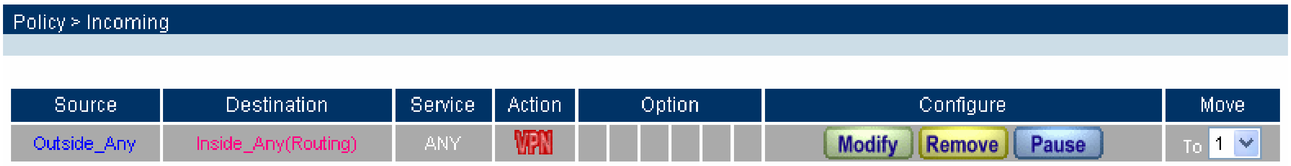
Outgoing Policy:



Policy > Outgoing

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	VPN		Modify Remove Pause	To 1
Inside_Any	Outside_Any	ANY	✓		Modify Remove Pause	To 2

Incoming Policy:



Policy > Incoming

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Inside_Any(Routing)	ANY	VPN		Modify Remove Pause	To 1

Example 4. Create a VPN connection between Content Security Gateway and PLANET VRT-311 VPN Router.

Preparation Task:

Company A External IP is 210.66.155.90

Internal IP is 192.168.10.X

Company B External IP is 210.66.155.92

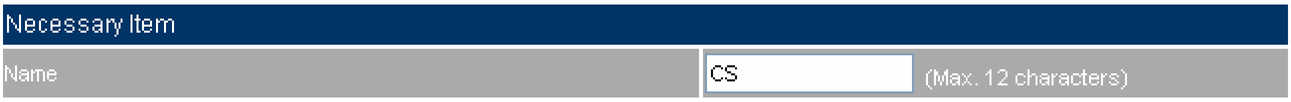
Internal IP is 192.168.20.X

To Allow Company A, 192.168.10.100 create a VPN connection with company B, 192.168.20.100 for downloading the sharing file.

The Gateway of Company A is 192.168.10.1. The settings of company A are as the following.

Step 1. Enter the default IP of Company A's Content Security Gateway, 192.168.10.1. Click VPN in the menu bar on the left hand side, and then select the sub-select IPSec Autokey. Click Add.

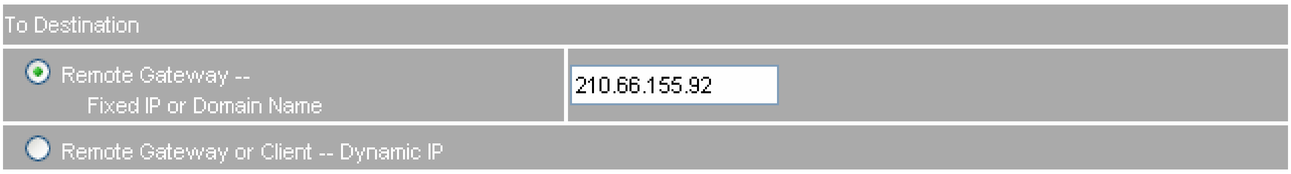
Step 2. Enter the VPN name, VPN_A in IPSec Autokey window.



Necessary Item

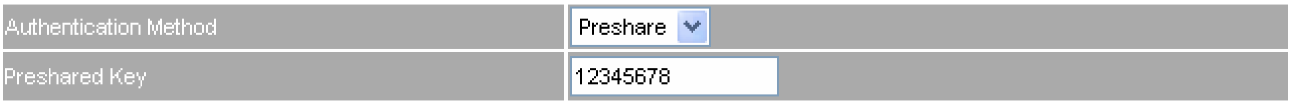
Name	CS (Max. 12 characters)

Step 3. In To Destination table, choose Remote Gateway-Fixed IP or Domain Name, enter the IP address desired to be connected.



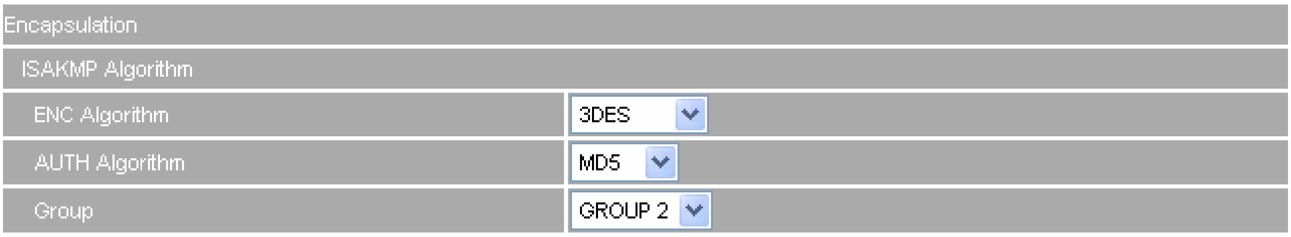
To Destination	
● Remote Gateway -- Fixed IP or Domain Name	210.66.155.92
○ Remote Gateway or Client -- Dynamic IP	

Step 4. In Authentication Method Table enters the Preshared Key.



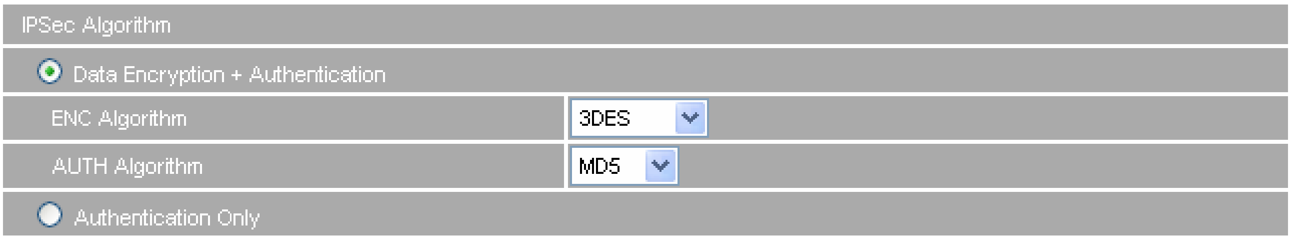
Authentication Method	Preshare
Preshared Key	12345678

Step 5. In Encapsulation or Authentication table, choose ISAKMP Algorithm. For communication via VPN, we choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm. And select Group 2 to connect.



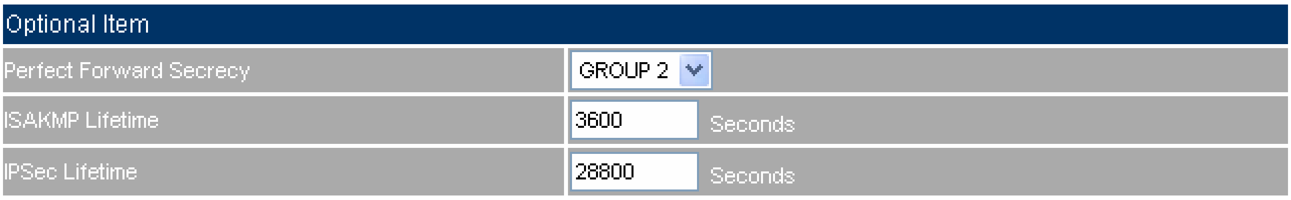
Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	3DES
AUTH Algorithm	MD5
Group	GROUP 2

Step 6. In IPSec Algorithm Table, choose Data Encryption + Authentication. We choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm.



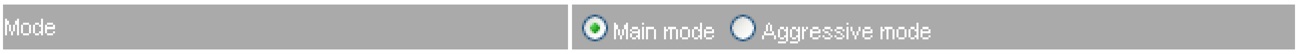
IPSec Algorithm	
● Data Encryption + Authentication	
ENC Algorithm	3DES
AUTH Algorithm	MD5
○ Authentication Only	

Step 7. Choose GROUP 2 as the Perfect Forward Secrecy setting, and leave the default setting with 28800 seconds in IPSec Lifetime and 3600 seconds for ISAKMP Lifetime.



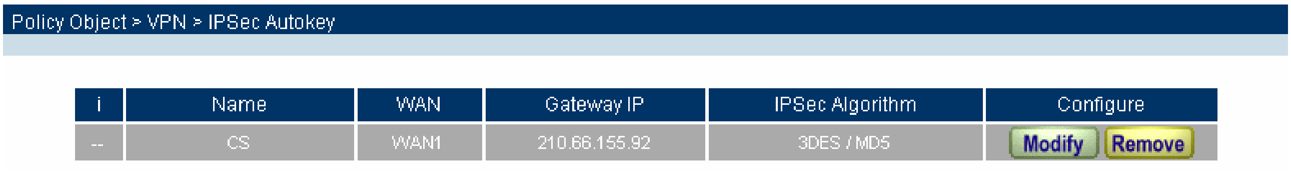
Optional Item	
Perfect Forward Secrecy	GROUP 2
ISAKMP Lifetime	3600 Seconds
IPSec Lifetime	28800 Seconds

Step 8. Select main mode as the algorithm.



Mode	● Main mode ○ Aggressive mode

Step 9. Click OK to finish the IPSec Aotukey setting of Company A.

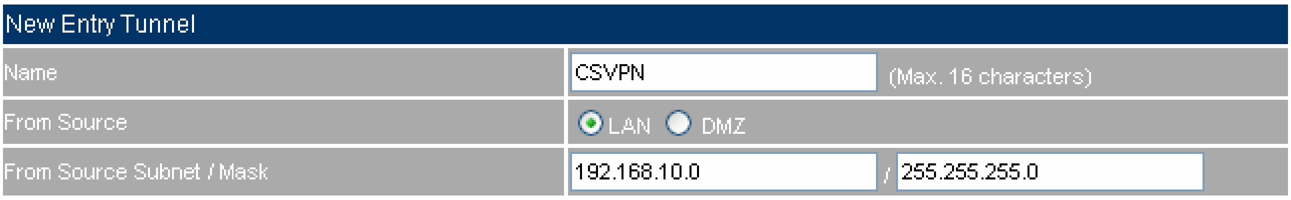


Policy Object > VPN > IPSec Autokey

i	Name	WAN	Gateway IP	IPSec Algorithm	Configure
--	CS	WAN1	210.66.155.92	3DES / MD5	Modify Remove

Step 10. Click Tunnel and press New Entry to configure the further setting.

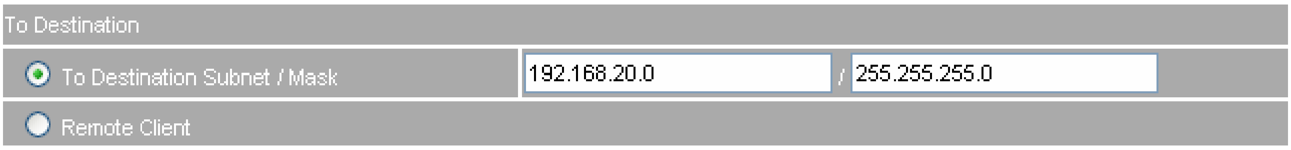
Step 11. Enter Site_A as the new tunnel name, and select LAN interface as the VPN source. Fill LAN IP subnet 192.168.10.0 with subnet mask IP 255.255.255.0.



New Entry Tunnel

Name	CSVPN (Max. 16 characters)
From Source	● LAN ○ DMZ
From Source Subnet / Mask	192.168.10.0 / 255.255.255.0

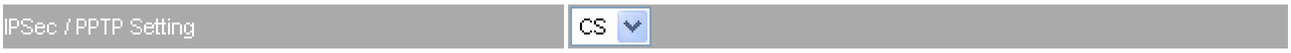
Step 12. In To Destination table, fill company B's subnet IP and mask, 192.168.20.0 and 255.255.255.0 respectively.



To Destination

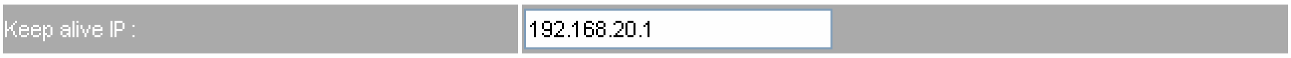
● To Destination Subnet / Mask	192.168.20.0 / 255.255.255.0
○ Remote Client	

Step 13. In IPSec /PPTP Setting, select CS as the available tunnel.



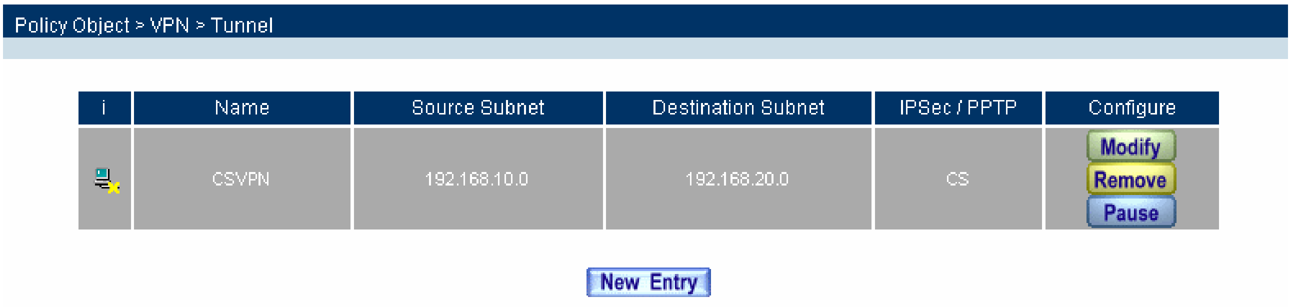
IPSec / PPTP Setting	CS

Step 14. Fill company B's gateway IP 192.168.20.1 in Keep alive IP to keep VPN tunnel connecting.



Keep alive IP :	192.168.20.1

Step 15. Click OK to finish the Tunnel setting of Company A.

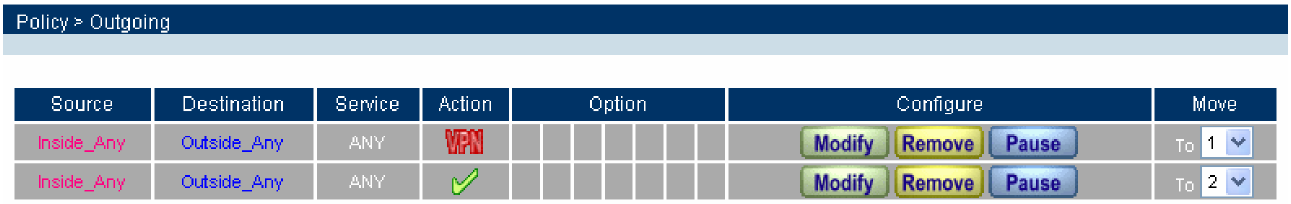


Policy Object > VPN > Tunnel

i	Name	Source Subnet	Destination Subnet	IPSec / PPTP	Configure
	CSVPN	192.168.10.0	192.168.20.0	CS	Modify Remove Pause

Step 16. If you want to configure bi-direction VPN connection, you should enable Tunnel setting in Outgoing and Incoming Policy.

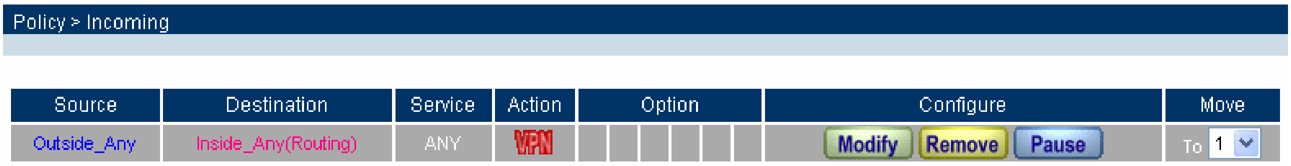
Outgoing Policy:



Policy > Outgoing

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	VPN		Modify Remove Pause	To 1
Inside_Any	Outside_Any	ANY	✓		Modify Remove Pause	To 2

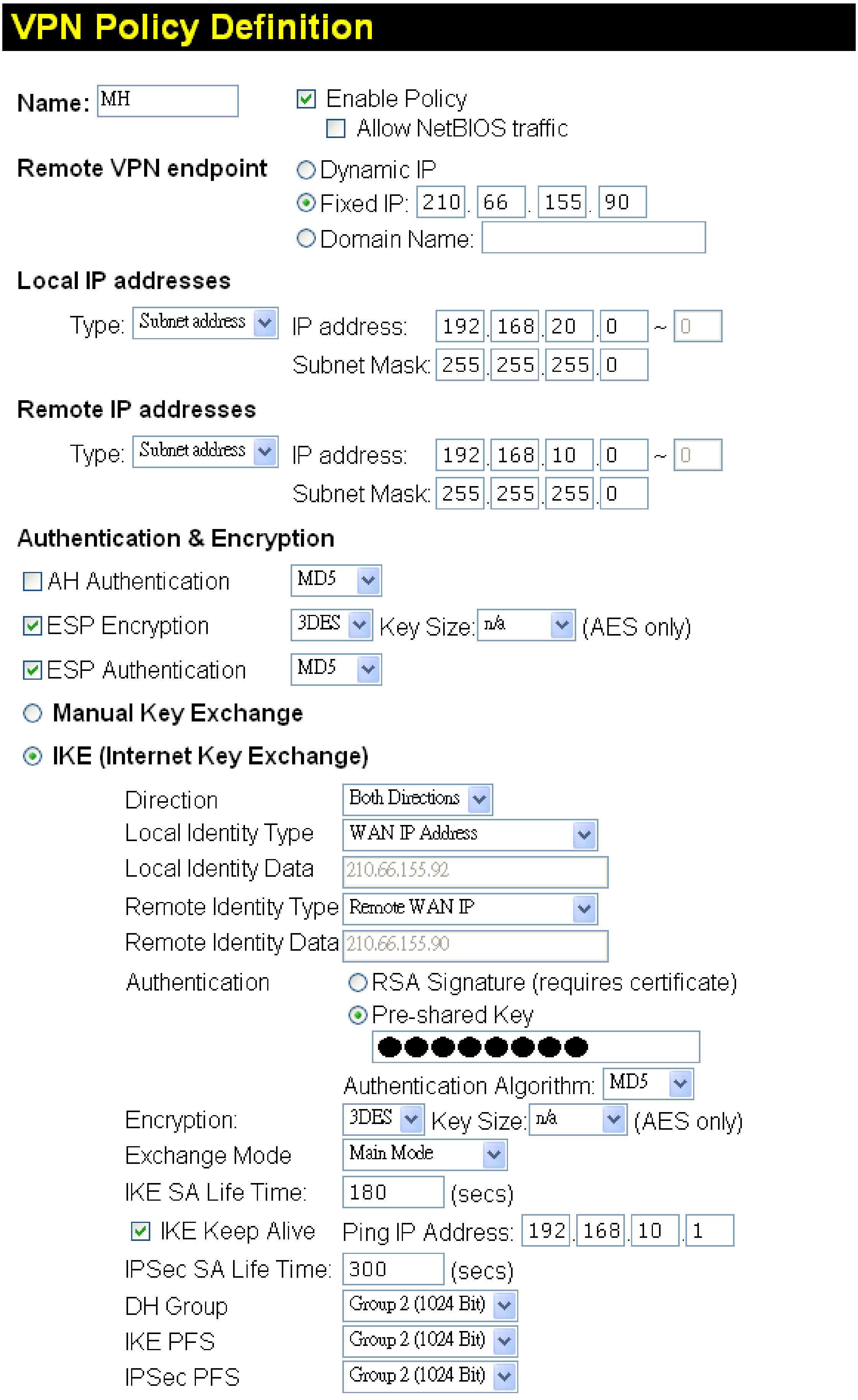
Incoming Policy:



Policy > Incoming

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Inside_Any(Routing)	ANY	VPN		Modify Remove Pause	To 1

Step 2: Configure VRT-311 VPN policy as the following:



VPN Policy Definition

Name: MH

☑ Enable Policy

☐ Allow NetBIOS traffic

Remote VPN endpoint

○ Dynamic IP

● Fixed IP: 210 . 66 . 155 . 90

○ Domain Name:

Local IP addresses

Type: Subnet address — IP address: 192 . 168 . 20 . 0 ~ 0

Subnet Mask: 255 . 255 . 255 . 0

Remote IP addresses

Type: Subnet address — IP address: 192 . 168 . 10 . 0 ~ 0

Subnet Mask: 255 . 255 . 255 . 0

Authentication & Encryption

☐ AH Authentication — MD5

☑ ESP Encryption — 3DES — Key Size: n/a (AES only)

☑ ESP Authentication — MD5

○ Manual Key Exchange

● IKE (Internet Key Exchange)

Direction: Both Directions

Local Identity Type: WAN IP Address

Local Identity Data: 210.66.155.92

Remote Identity Type: Remote WAN IP

Remote Identity Data: 210.66.155.90

Authentication: ○ RSA Signature (requires certificate)

● Pre-shared Key

●●●●●●●●

Authentication Algorithm: MD5

Encryption: 3DES — Key Size: n/a (AES only)

Exchange Mode: Main Mode

IKE SA Life Time: 180 (secs)

☑ IKE Keep Alive — Ping IP Address: 192 . 168 . 10 . 1

IPSec SA Life Time: 300 (secs)

DH Group: Group 2 (1024 Bit)

IKE PFS: Group 2 (1024 Bit)

IPSec PFS: Group 2 (1024 Bit)

4.4 Policy

This section provides the Administrator with facilities to sent control policies for packets with different source IP addresses, source ports, destination IP addresses, and destination ports. Control policies decide whether packets from different network objects, network services, and applications are able to pass through the Content Security Gateway.

What is Policy?

The device uses policies to filter packets. The policy settings are: source address, destination address, services, permission, packet log, packet statistics, and flow alarm. Based on its source addresses, a packet can be categorized into:

(1)Outgoing: a client is in the LAN networks while a server is in the WAN networks.

(2) Incoming, a client is in the WAN networks, while a server is in the LAN networks.

(3) To DMZ: a client is either in the LAN networks or in the WAN networks while, server is in DMZ.

(4) From DMZ, a client is in DMZ while server is either in the LAN networks or in the WAN networks.

How do I use Policy?

The policy settings are source addresses, destination addresses, services, permission, log, statistics, and flow alarm. Among them, source addresses, destination addresses and IP mapping addresses have to be defined in the **Address** menu in advance. Services can be used directly in setting up policies, if they are in the Pre-defined Service menu. Custom services need to be defined in the **Custom** menu before they can be used in the policy settings.

If the destination address of an incoming policy is a Mapped IP address or a Virtual Server address, then the address has to be defined in the **Virtual Server** section instead of the **Address** section.

Policy Directions:

Step 1. In **Address**, set names and addresses of source networks and destination networks.

Step 2. In **Service**, set services.

Step 3. In **Virtual Server**, set names and addresses of mapped IP or virtual server (only applied to **Incoming policies**).

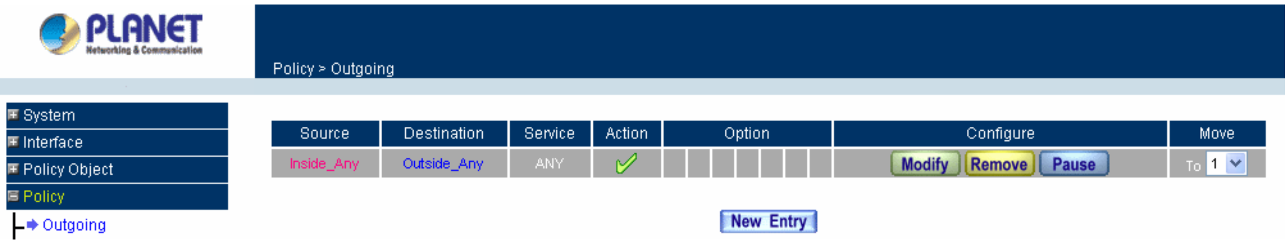
Step 4. Set control policies in **Policy.**

4.4.1 Outgoing

This section describes steps to create policies for packets and services from the LAN network to the WAN network.

Entering the Outgoing window:

Click **Policy** on the left hand side menu bar, then click **Outgoing** under it. A window will appear with a table displaying currently defined Outgoing policies.



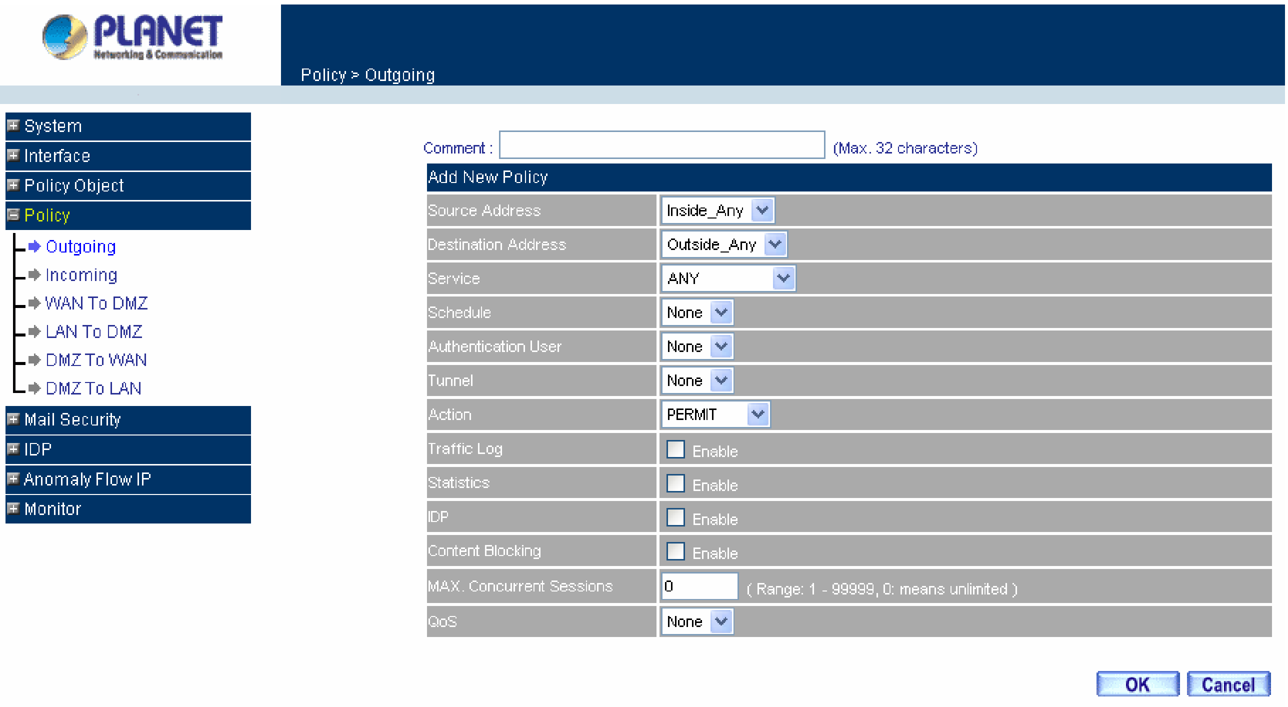
Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	✓		Modify Remove Pause	To 1

The fields in the Outgoing window are:

- **Source:** Source network addresses that are specified in the LAN section of **Address** menu, or all the LAN network addresses.
- **Destination:** Destination network addresses that are specified in the WAN section of the Address menu, or all of the WAN network addresses.
- **Service:** Specify services provided by WAN network servers.
- **Action:** Control actions to permit or deny packets from LAN networks to WAN network travelling through the Content Security Gateway.
- **Option:** Specify the monitoring functions on packets from LAN networks to WAN networks travelling through the Content Security Gateway.
- **Configure:** Modify settings.
- **Move:** This sets the priority of the policies, number 1 being the highest priority.

Adding a new Outgoing Policy

Step 1: Click on the New Entry button and the Add New Policy window will appear.



Comment : (Max. 32 characters)

Add New Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
Tunnel	None
Action	PERMIT
Traffic Log	□ Enable
Statistics	□ Enable
IDP	□ Enable
Content Blocking	□ Enable
MAX. Concurrent Sessions	0 (Range: 1 - 99999, 0: means unlimited)
QoS	None

Step 2: Configure all the parameters.

Source Address: Select the name of the LAN network from the drop down list. The drop down list contains the names of all LAN networks defined in the LAN section of the **Address** menu. To create a new source address, please go to the LAN section under the **Address** menu.

Destination Address: Select the name of the WAN network from the drop down list. The drop down list contains the names of all WAN networks defined in the WAN section of the **Address** window. To create a new destination address, please go to the WAN section under the **Address** menu.

Service: Specified services provided by WAN net work servers. These are services/application that are allowed to pass from the LAN network to the WAN network. Choose ANY for all services.

Schedule: Select the item listed in the schedule to enable the policy to automatically execute the function in a certain time and range.

Authentication User: Select the item listed in the Authentication User to enable the policy to automatically execute the function in a certain time and range.

Tunnel: Select the specific VPN tunnel to enable the VPN traffic in Policy rule.

Action: Select Permit or Deny ALL from the drop down list to allow or reject the packets travelling between the source network and the destination network.

Traffic Log: Select Enable to enable flow monitoring.

Statistics: Select Enable to enable flow statistics.

IDP: Check to enable IDP feature.

Content Blocking: Select Enable to enable Content Blocking.

Max. Concurrent Sessions: The maximum concurrent sessions that allows passing through CS-500. 0 means it is unlimited.

QoS: Select the item listed in the QoS to enable the policy to automatically execute the function in a certain time and range.

Step 3: Click **OK** to add a new outgoing policy; or click **Cancel** to cancel adding a new outgoing policy.

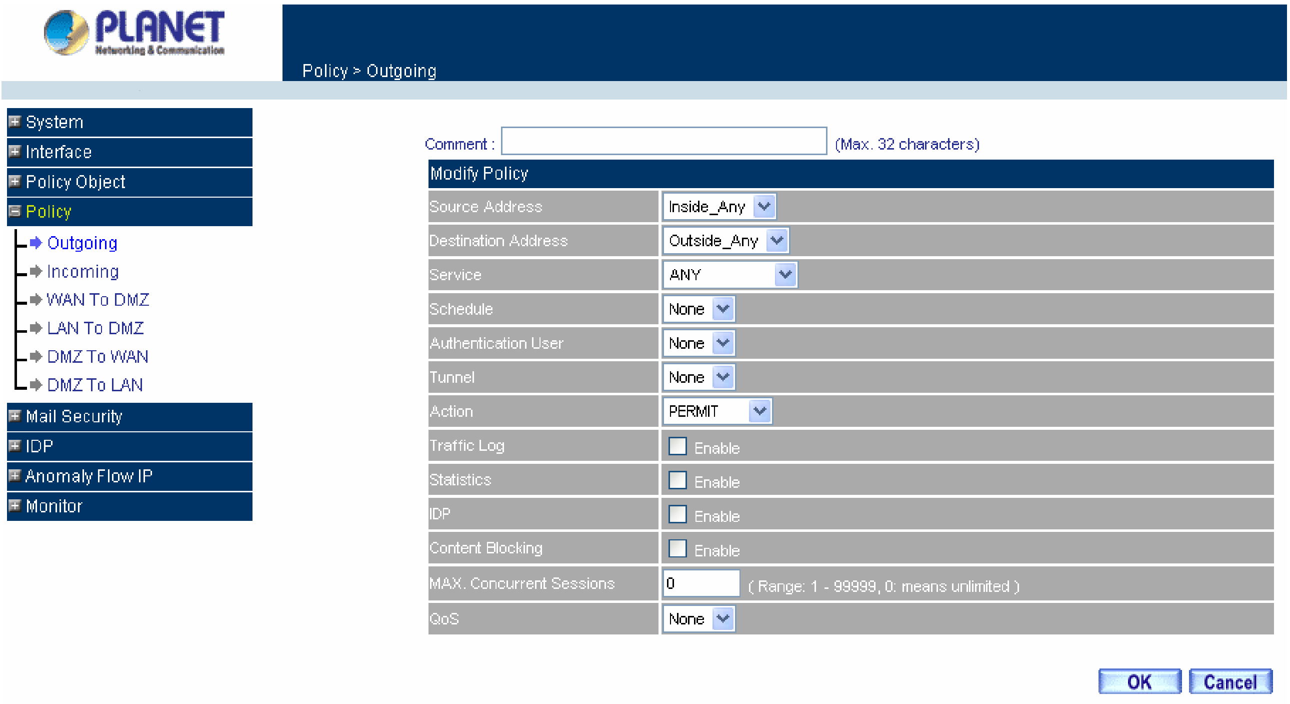
Modifying an Outgoing policy

Step 1: In the **Outgoing** policy section, locate the name of the policy desired to be modified and click its corresponding Modify option under the Configure field.

Step 2: In the **Modify Policy** window, fill in new settings.

NOTE: To change or add selections in the drop-down list for source or destination address, go to the section where the selections are setup. (Source Address→LAN of **Address** menu; Destination Address → WAN of **Address** menu; Service→ [Pre-defined], [Custom] or Group under **Service**).

Step 3: Click **OK** to do confirm modification or click **Cancel** to cancel it.



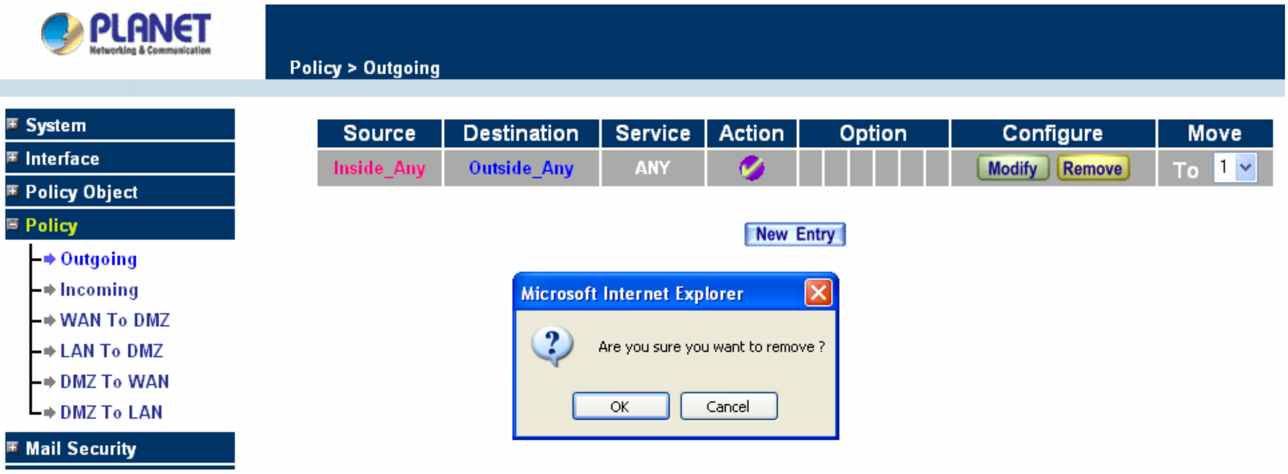
Comment : (Max. 32 characters)

Modify Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
Tunnel	None
Action	PERMIT
Traffic Log	□ Enable
Statistics	□ Enable
IDP	□ Enable
Content Blocking	□ Enable
MAX. Concurrent Sessions	0 (Range: 1 - 99999, 0: means unlimited)
QoS	None

Removing the Outgoing Policy

Step 1. In the **Outgoing** policy section, locate the name of the policy desired to be removed and click its corresponding **Remove** option in the **Configure** field.

Step 2. In the **Remove** confirmation dialogue box, click **OK** to remove the policy or click **Cancel** to cancel removing.



Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	✓		Modify Remove	To 1

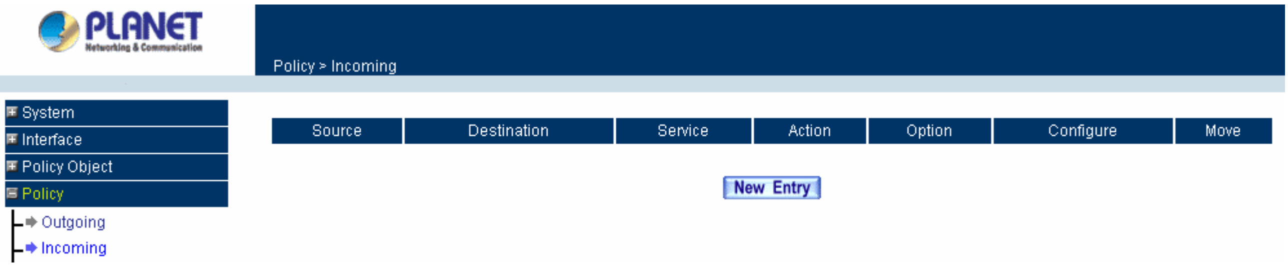
Are you sure you want to remove ?

4.4.2 Incoming

This section describes steps to create policies for packets and services from the WAN network to the LAN network including Mapped IP and Virtual Server.

Enter Incoming window

Step 1: Click **Incoming** under the **Policy** menu to enter the Incoming window. The Incoming table will display current defined policies from the WAN network to assigned Mapped IP or Virtual Server.



Policy > Incoming

Source	Destination	Service	Action	Option	Configure	Move

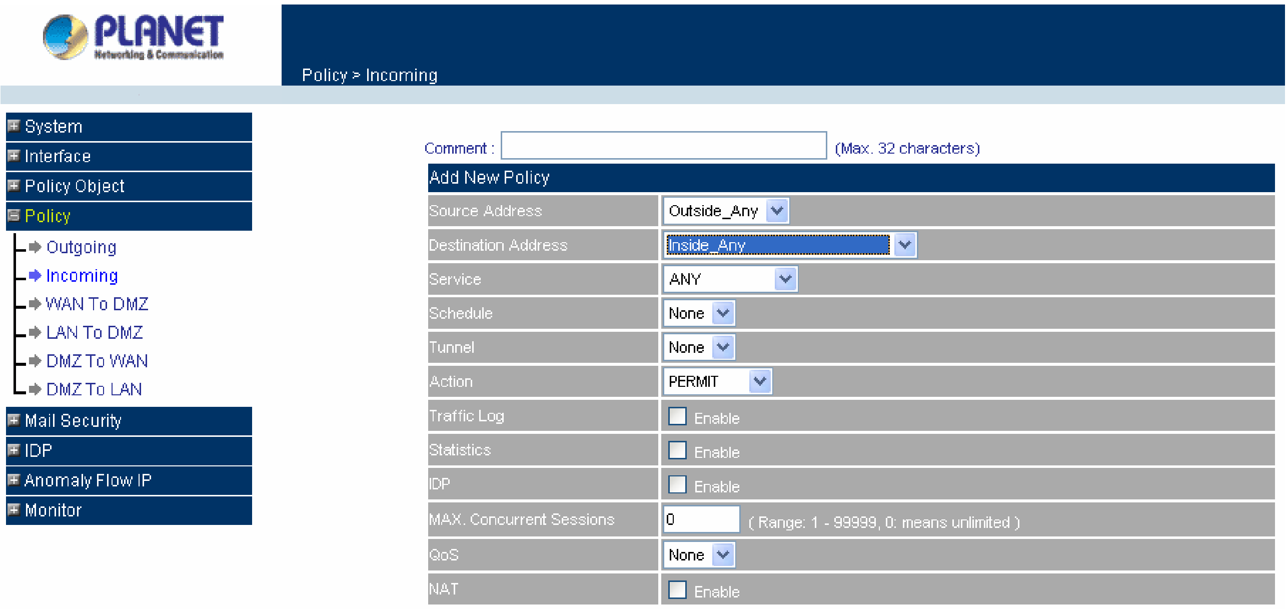
New Entry

Step 2: The fields of the **Incoming** window are:

- **Source:** Source networks which are specified in the **WAN** section of the **Address** menu, or all the WAN network addresses.
- **Destination:** Destination networks, which are IP Mapping addresses or Virtual server network addresses created in **Virtual Server** menu.
- **Service:** Services supported by Virtual Servers (or Mapped IP).
- **Action:** Control actions to permit or deny packets from WAN networks to Virtual Server/Mapped IP travelling through the device.
- **Option:** Specify the monitoring functions on packets from WAN networks to Virtual Server/Mapped IP travelling through the Content Security Gateway.
- **Configure:** Modify settings or remove incoming policy.
- **Move:** This sets the sequence of the policies, number 1 being the first policy to proceed.

Adding an Incoming Policy

Step 1: Under **Incoming** of the **Policy** menu, click the New Entry button.



Policy > Incoming

Comment : (Max. 32 characters)

Add New Policy	
Source Address	Outside_Any
Destination Address	Inside_Any
Service	ANY
Schedule	None
Tunnel	None
Action	PERMIT
Traffic Log	□ Enable
Statistics	□ Enable
IDP	□ Enable
MAX. Concurrent Sessions	0 (Range: 1 - 99999, 0: means unlimited)
QoS	None
NAT	□ Enable

Step 2: Configure the parameters

Source Address: Select names of the WAN networks from the drop down list. The drop down list contains the names of all WAN networks defined in the WAN section of the Address menu. To create a new source address, please go to the LAN section under the Address menu.

Destination Address: Select names of the LAN networks from the drop down list. The drop down list contains the names of IP mapping addresses specified in the **Mapped IP** or the **Virtual Server** sections of **Virtual Server** menu. To create a new destination address, please go to the **Virtual Server** menu.

Service: Specified services provided by LAN network servers. These are services / application that are allowed to pass from the network to the LAN network. Choose ANY for all services.

Schedule: Select the item listed in the schedule to enable the policy to automatically execute the function in a certain time and range.

Tunnel: Select the specific VPN tunnel to enable the VPN traffic in Policy rule.

Action: Select Permit or Deny ALL from the drop down list to allow or reject the packets travelling between the specified WAN network and Virtual Server/Mapped IP.

Traffic Log: Select Enable to enable flow monitoring.

Statistics: Select Enable to enable flow statistics.

IDP: Check to enable IDP feature.

Max. Concurrent Sessions: The maximum concurrent sessions that allows to pass through CS-500. 0 means it is unlimited.

QoS: Select the item listed in the QoS to enable the policy to automatically execute the function in a certain time and range.

NAT: Select enable to replace Internet user's IP address with LAN interface IP, in order to allow Internet user to access LAN resource if the LAN server only allows to be accessed with the same IP subnet.

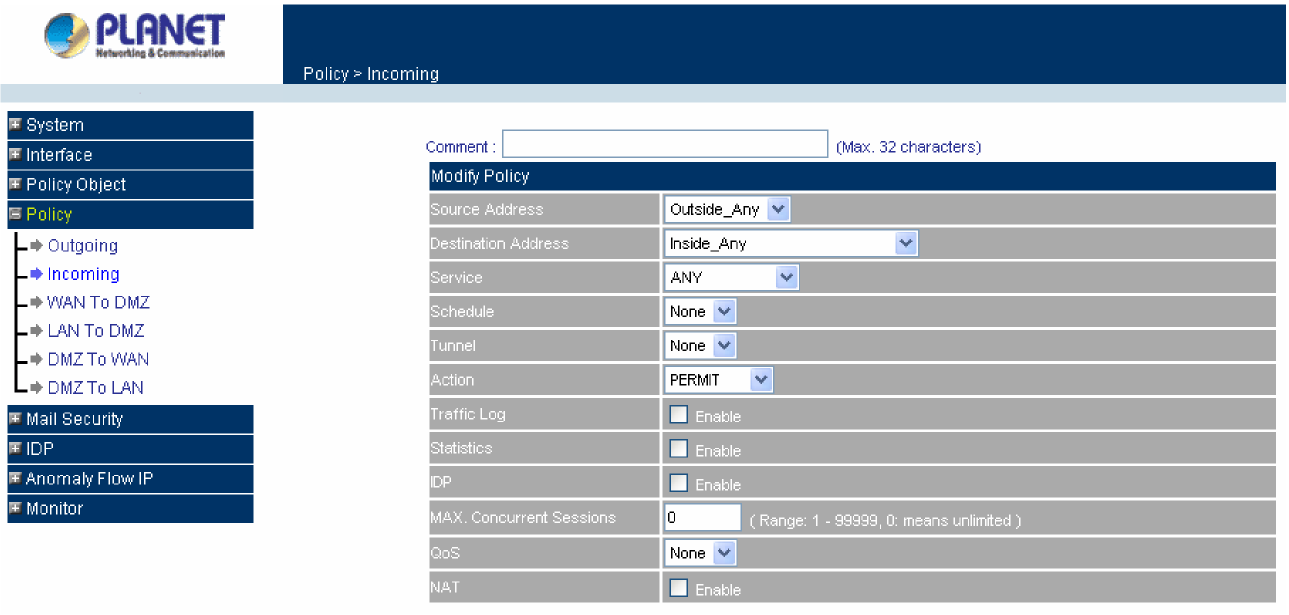
Step 3: Click **OK** to add new policy or click **Cancel** to cancel adding new incoming policy.

Modifying Incoming Policy

Step 1: In the **Incoming** window, locate the name of policy desired to be modified and click its corresponding Modify option in the Configure field.

Step 2: In the Modify Policy window, fill in new settings.

Step 3: Click **OK** to save modifications or click **Cancel** to cancel modifications.



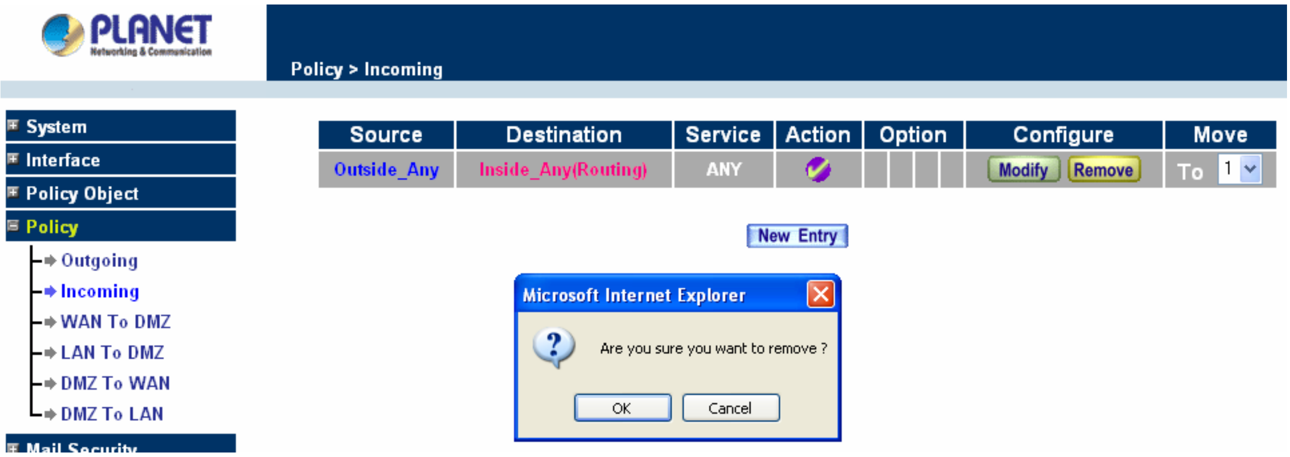
Comment : (Max. 32 characters)

Modify Policy	
Source Address	Outside_Any
Destination Address	Inside_Any
Service	ANY
Schedule	None
Tunnel	None
Action	PERMIT
Traffic Log	□ Enable
Statistics	□ Enable
IDP	□ Enable
MAX. Concurrent Sessions	0 (Range: 1 - 99999, 0: means unlimited)
QoS	None
NAT	□ Enable

Removing an Incoming Policy

Step 1: In the **Incoming** window, locate the name of policy desired to be removed and click its corresponding [**Remove**] in the Configure field.

Step 2: In the Remove confirmation window, click **Ok** to remove the policy or click **Cancel** to cancel removing.



Source	Destination	Service	Action	Option				Configure	Move
Outside_Any	Inside_Any(Routing)	ANY	✓					Modify Remove	To 1

Microsoft Internet Explorer

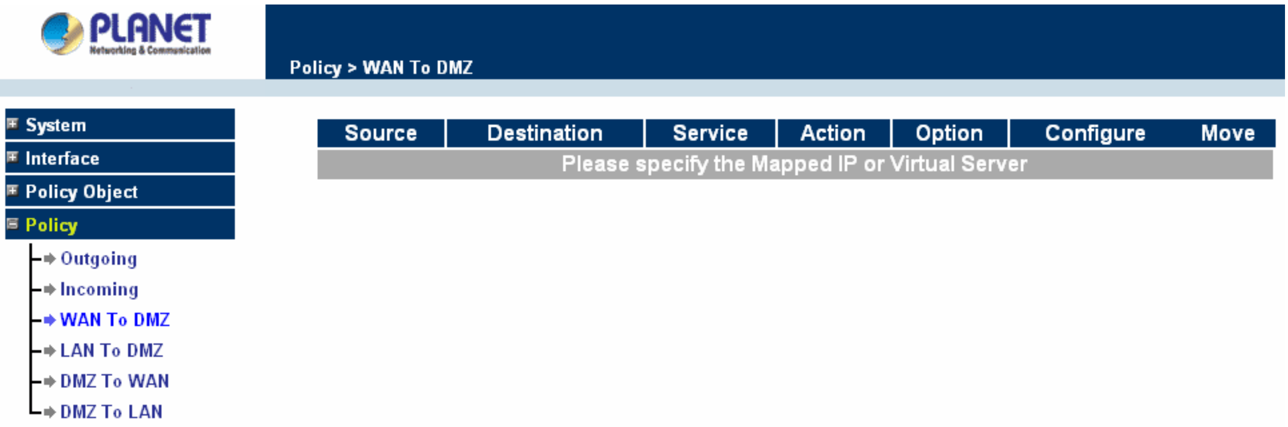
Are you sure you want to remove ?

4.4.3 WAN To DMZ & LAN To DMZ

This section describes steps to create policies for packets and services from the WAN networks to the DMZ networks. Please follow the same procedures for LAN networks to DMZ networks.

Enter [WAN To DMZ] or [LAN To DMZ] window:

Click **WAN To DMZ** under **Policy** menu to enter the **WAN To DMZ** window. The WAN To DMZ table will show up displaying currently defined policies. Before to set up **WAN To DMZ** rule, you need to create **Virtual Server** or **Mapped IP** first.



Source	Destination	Service	Action	Option	Configure	Move
Please specify the Mapped IP or Virtual Server						

The fields in WAN To DMZ window:

Source: Source networks, which are addresses specified in the **WAN** section of the **Address** menu, or all the WAN network addresses.

Destination: Destination networks, which are addresses specified in **DMZ** section of the **Address** menu and **Mapped IP** addresses of the **Virtual Server** menu.

Service: Services supported by servers in DMZ network.

Action: Control actions, to permit or deny packets from WAN networks to DMZ travelling through the Content Security Gateway.

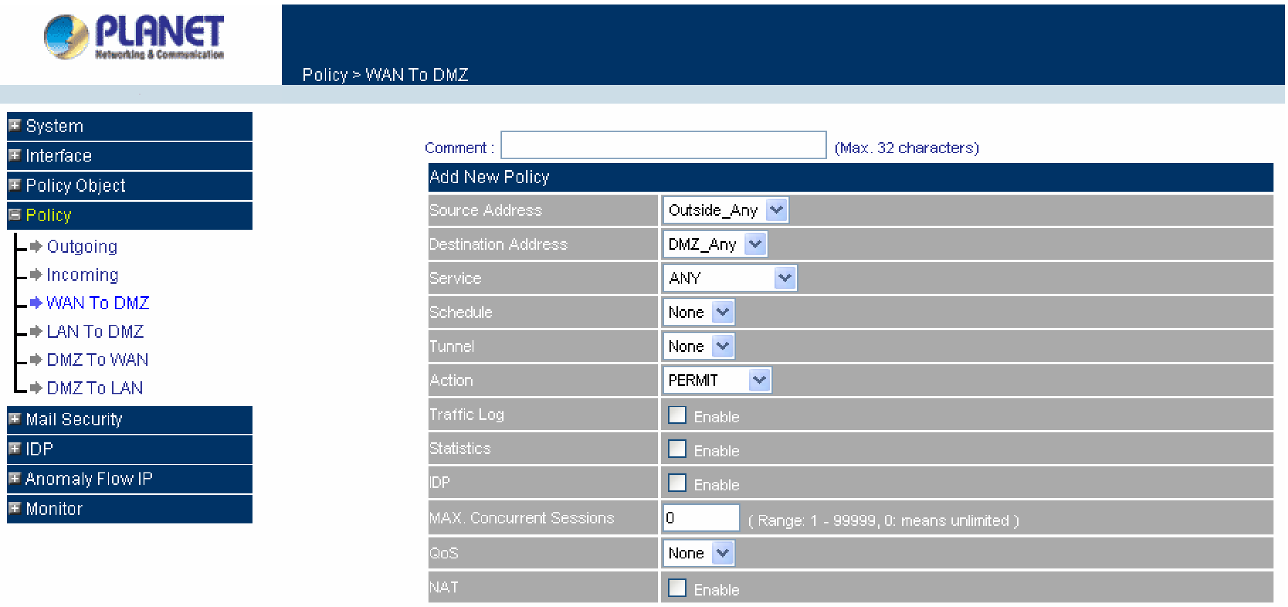
Option: Specify the monitoring functions of packets from WAN network to DMZ network travelling through Content Security Gateway.

Configure: Modify settings or remove policies.

Move: This sets the priority of the policies, number 1 being the highest priority.

Adding a new WAN To DMZ Policy:

Step 1: Click the New Entry button and the Add New Policy window will appear.



Comment : (Max. 32 characters)

Add New Policy	
Source Address	Outside_Any
Destination Address	DMZ_Any
Service	ANY
Schedule	None
Tunnel	None
Action	PERMIT
Traffic Log	□ Enable
Statistics	□ Enable
IDP	□ Enable
MAX. Concurrent Sessions	0 (Range: 1 - 99999, 0: means unlimited)
QoS	None
NAT	□ Enable

Step 2: Configure the parameters.

Source Address: Select names of the WAN networks from the drop down list. The drop down list contains the names of all WAN networks defined in the **WAN** section of the **Address** menu. To create a new source address, please go to the **LAN** section under the **Address** menu.

Destination Address: Select the name of the DMZ network from the drop down list. The drop down list contains the names of the DMZ network created in the **Address** menu. It will also contain Mapped IP addresses from the **Virtual Server** menu that were created for the DMZ network. To create a new destination address, please go to the **Virtual Server** menu. (Please refer to the sections entitled **Address** and **Virtual Server** for details)

Service: Select a service from drop down list. The drop down list will contain services defined in the **Custom** or **Group** section under the **Service** menu. These are services/application that are allowed to pass from the WAN network to the DMZ network. Choose ANY for all services. To add or modify these services, please go to the **Service** menu. (Please refer to the section entitled **Services** for details)

Schedule: Select the item listed in the schedule to enable the policy to automatically execute the function in a certain time and range.

Tunnel: Select the specific VPN tunnel to enable the VPN traffic in Policy rule.

Action: Select Permit or Deny ALL from the drop down list to allow or reject the packets travelling from the specified WAN network to the DMZ network.

Traffic Log: Select Enable to enable flow monitoring.

Statistics: Select Enable to enable flow statistics.

IDP: Check to enable IDP feature.

Max. Concurrent Sessions: The maximum concurrent sessions that allows to pass through CS-500. 0 means it is unlimited.

QoS: Select the item listed in the QoS to enable the policy to automatically execute the function in a certain time and range.

NAT: Select enable to replace Internet user's IP address with DMZ interface IP, in order to allow Internet user to access DMZ resource if the DMZ server only allows to be accessed with the same IP subnet.

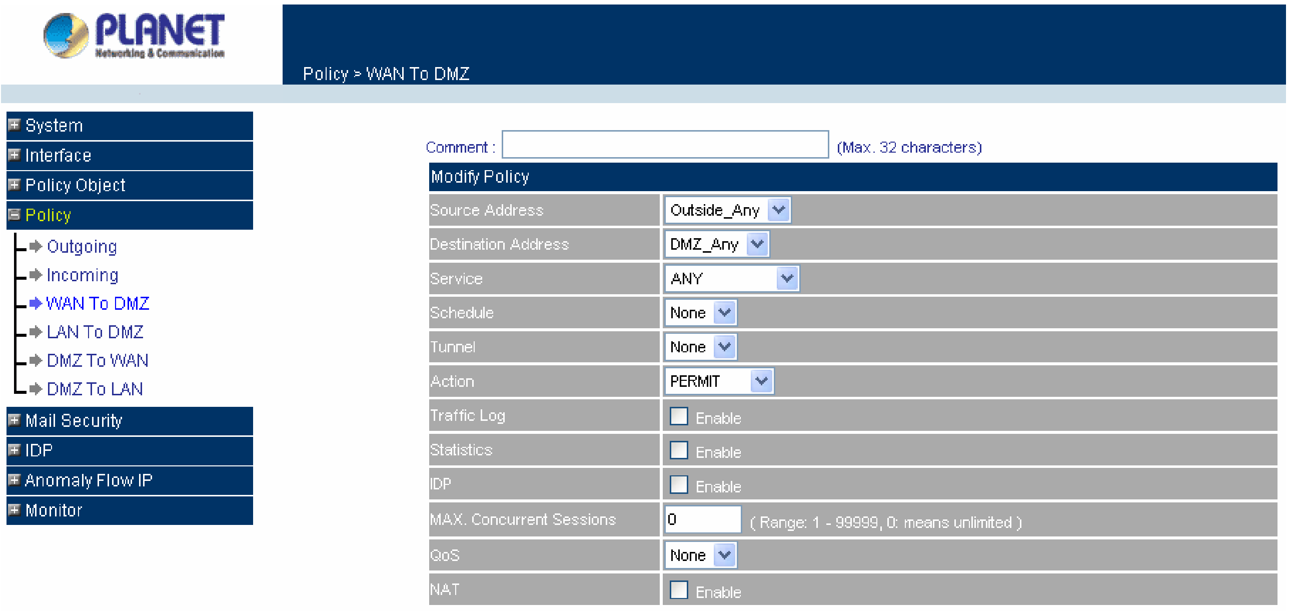
Step 3: Click **OK**.

Modifying a WAN To DMZ policy:

Step 1: In the **WAN To DMZ** window, locate the name of policy desired to be modified and click its corresponding **Modify** option in the **Configure** field.

Step 2: In the **Modify Policy** window, fill in new settings.

Step 3: Click **OK** to do save modifications.



Policy > WAN To DMZ

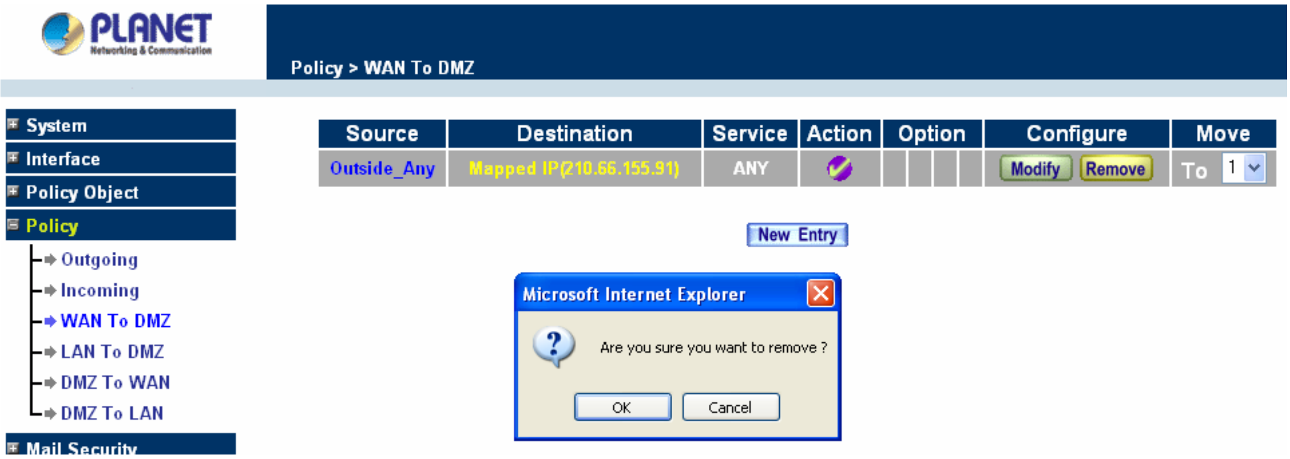
Comment : (Max. 32 characters)

Modify Policy	
Source Address	Outside_Any
Destination Address	DMZ_Any
Service	ANY
Schedule	None
Tunnel	None
Action	PERMIT
Traffic Log	□ Enable
Statistics	□ Enable
IDP	□ Enable
MAX. Concurrent Sessions	0 (Range: 1 - 99999, 0: means unlimited)
QoS	None
NAT	□ Enable

Removing a WAN To DMZ Policy:

Step 1: In the **WAN To DMZ** window, locate the name of policy desired to be removed and click its corresponding **Remove** option in the **Configure** field.

Step 2: In the **Remove** confirmation pop-up box, click **OK** to remove the policy.



Policy > WAN To DMZ

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Mapped IP(210.66.155.91)	ANY			Modify Remove	To 1

Microsoft Internet Explorer

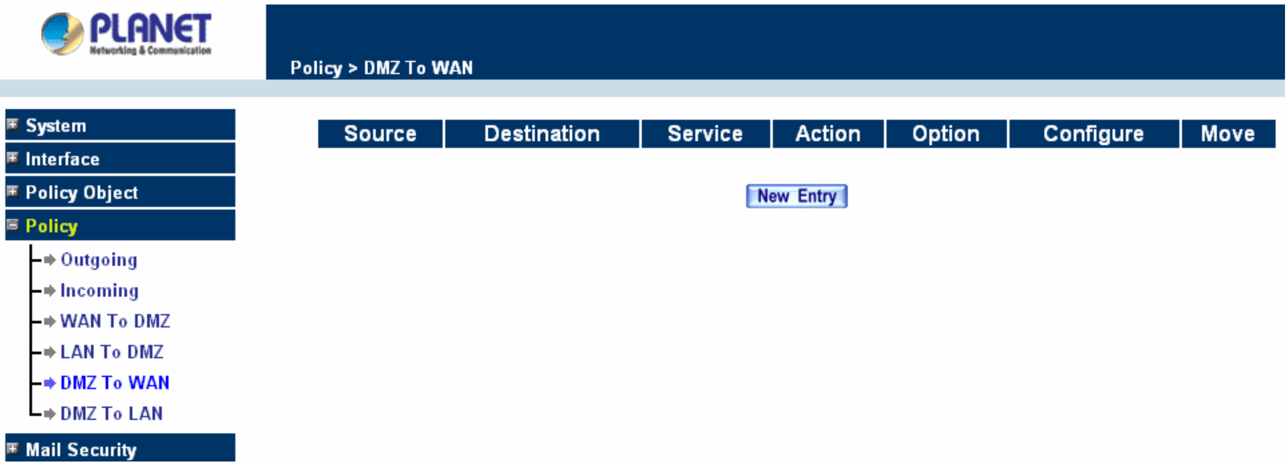
Are you sure you want to remove ?

4.4.4 DMZ To WAN & DMZ To LAN

This section describes steps to create policies for packets and services from DMZ networks to WAN networks. Please follow the same procedures for DMZ networks to LAN networks.

Entering the DMZ To WAN window:

Click **DMZ To WAN** under **Policy** menu and the **DMZ To WAN** table appears displaying currently defined **DMZ To WAN** policies.



The fields in the DMZ To WAN window are:

Source: Source network addresses which are specified in the **DMZ** section of the **Address** window.

Destination: Destination networks, which is the WAN network address

Service: Services supported by Servers of WAN networks.

Action: Control actions, to permit or deny packets from the DMZ network to WAN networks travelling through the Content Security Gateway.

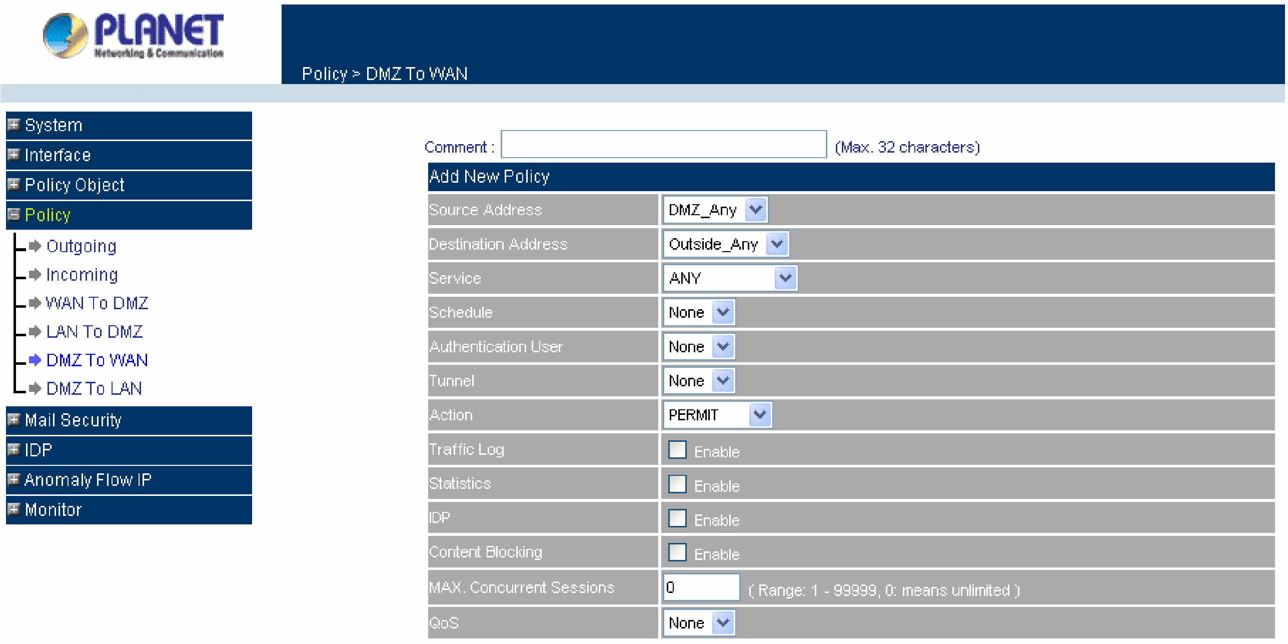
Option: Specify the monitoring functions on packets from the DMZ network to WAN networks travelling through the Content Security Gateway.

Configure: Modify settings or remove policies

Move: This sets the sequence of the policies, number 1 being the first policy to proceed.

Adding a DMZ To WAN Policy:

Step 1: Click the New Entry button and the Add New Policy window will appear.



Policy > DMZ To WAN

Comment : (Max. 32 characters)

Add New Policy	
Source Address	DMZ_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
Tunnel	None
Action	PERMIT
Traffic Log	□ Enable
Statistics	□ Enable
IDP	□ Enable
Content Blocking	□ Enable
MAX. Concurrent Sessions	0 (Range: 1 - 99999, 0: means unlimited)
QoS	None

Step 2: Configure the parameters.

Source Address: Select the name of the DMZ network from the drop down list. The drop down list will contain names of DMZ networks defined in **DMZ** section of the **Address** menu. To add a new source address, please go to the **DMZ** section under the **Address** menu.

Destination Address: Select the name of the WAN network from the drop down list. The drop down list lists names of addresses defined in **WAN** section of the **Address** menu. To add a new destination address, please go to **WAN** section of the **Address** menu.

Service: Select a service from drop down list. The drop down list will contain services defined in the **Custom** or **Group** section under the **Service** menu. These are services/application that are allowed to pass from the DMZ network to the WAN network. Choose ANY for all services. To add or modify these services, please go to the **Service** menu.

Schedule: Select the item listed in the schedule to enable the policy to automatically execute the function in a certain time and range.

Authentication User: Select the item listed in the Authentication User to enable the policy to automatically execute the function in a certain time and range.

Tunnel: Select the specific VPN tunnel to enable the VPN traffic in Policy rule.

Action: Select Permit or Deny ALL from the drop down list to allow or reject the packets travelling from the specified DMZ network to the WAN network.

Traffic Log: Select Enable to enable flow monitoring.

Statistics: Select Enable to enable flow statistics.

IDP: Check to enable IDP feature.

Content Blocking: Select Enable to enable Content Blocking.

Max. Concurrent Sessions: The maximum concurrent sessions that allows to pass through CS-500. 0 means it is unlimited.

QoS: Select the item listed in the QoS to enable the policy to automatically execute the function in a certain time and range.

Step 3: Click **OK** to add new policy or click **Cancel** to cancel adding.

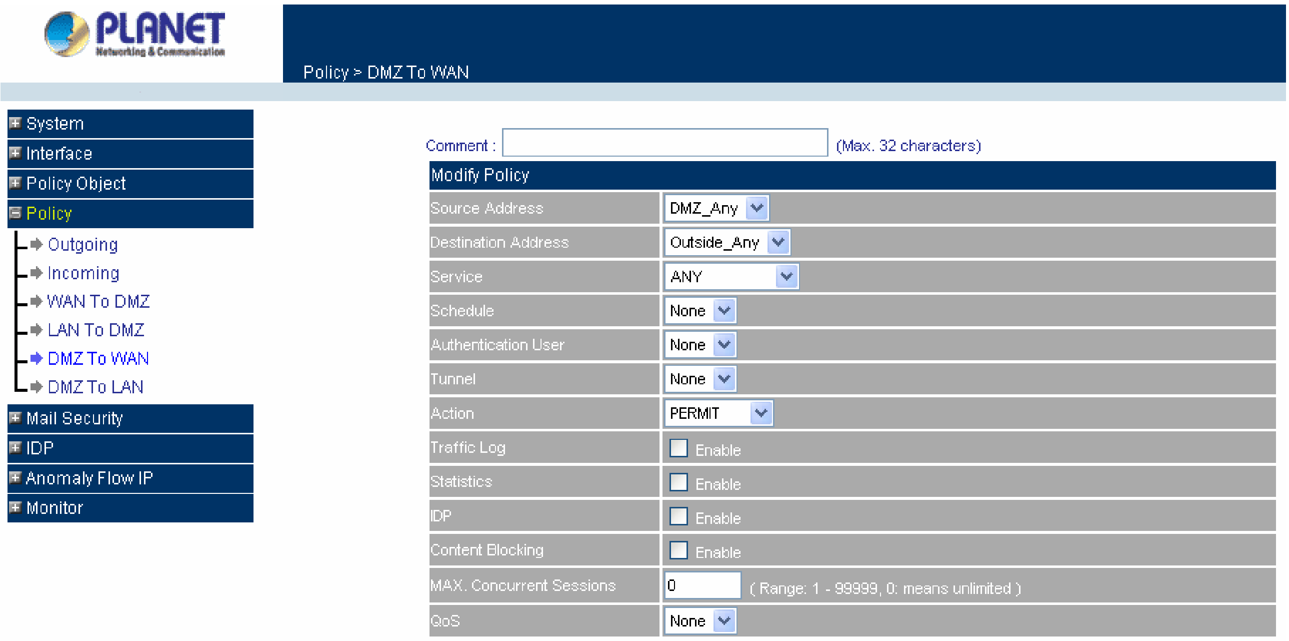
Modifying a DMZ To WAN policy:

Step 1: In the DMZ To WAN window, locate the name of policy desired to be modified and click its corresponding Modify option in the Configure field.

Step 2: In the Modify Policy window, fill in new settings.

NOTE: To change or add selections in the drop-down list, go to the section where the selections are setup. (Source Address → DMZ of Address; Destination Address →WAN, Service →Pre-defined Service, Custom or Group under Service.)

Step 3: Click OK to save modifications or click Cancel to cancel modifications.



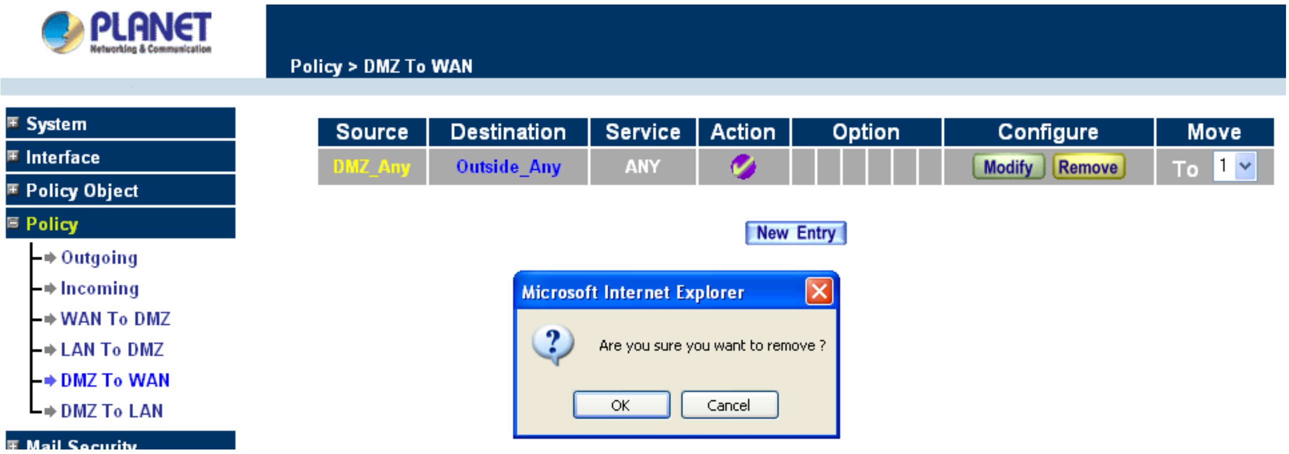
Comment : (Max. 32 characters)

Modify Policy	
Source Address	DMZ_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
Tunnel	None
Action	PERMIT
Traffic Log	□ Enable
Statistics	□ Enable
IDP	□ Enable
Content Blocking	□ Enable
MAX. Concurrent Sessions	0 (Range: 1 - 99999, 0: means unlimited)
QoS	None

Removing a DMZ To WAN Policy:

Step 1. In the **DMZ To WAN** window, locate the name of policy desired to be removed and click its corresponding Remove option in the Configure field.

Step 2. In the **Remove confirmation** dialogue box, click **OK.**



Source	Destination	Service	Action	Option	Configure	Move
DMZ_Any	Outside_Any	ANY			Modify Remove	To 1

Are you sure you want to remove ?

4.5 Mail Security

This section provides the Administrator to configure Mail Security rule for protecting client PC from virus and spam mail attacking. Meanwhile, CS-500 provides the ability to update virus pattern by schedule or manually, and it also provides auto-learning system to raise the rate of spam mail judging. For more detail information please check the related chapter.

4.5.1 Configure

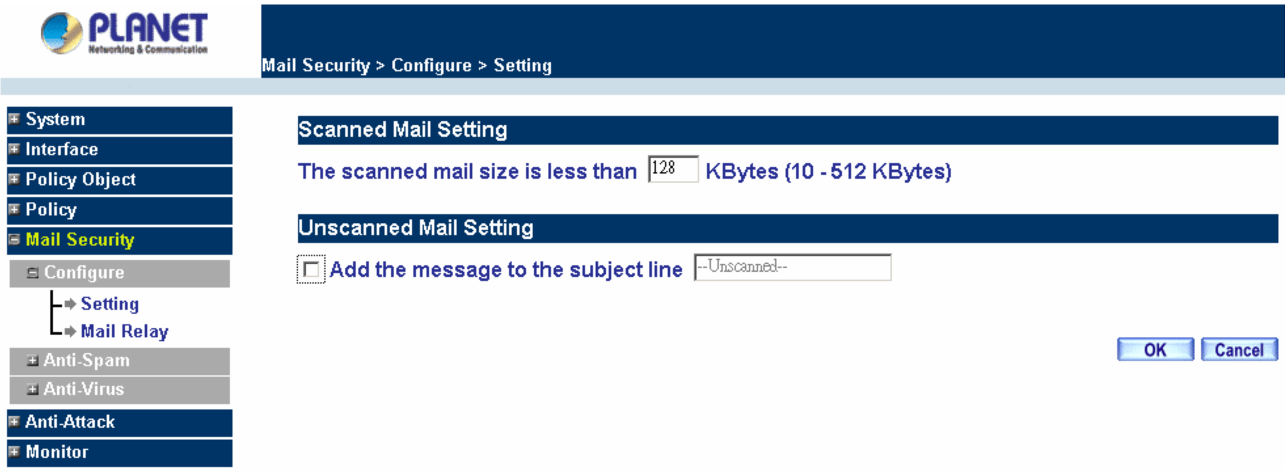
About the Mail Security Configure function, it means the dealing standard towards mail of CS-500. In this chapter, it is defined as Setting and Mail Relay.

Setting:

Define the required fields of setting:

Scanned Mail Setting: Setup to deal with the mail size in order to judge the mail should be scanned or not.

Unscanned Mail Setting: If the mail does not be scanned via CS-500, it can be marked an unscanned message in the mail subject. For example, if the mail size is less than the **Scanned Mail Setting**, when you receive mail you will find out the subject with the mark "Unscanned".



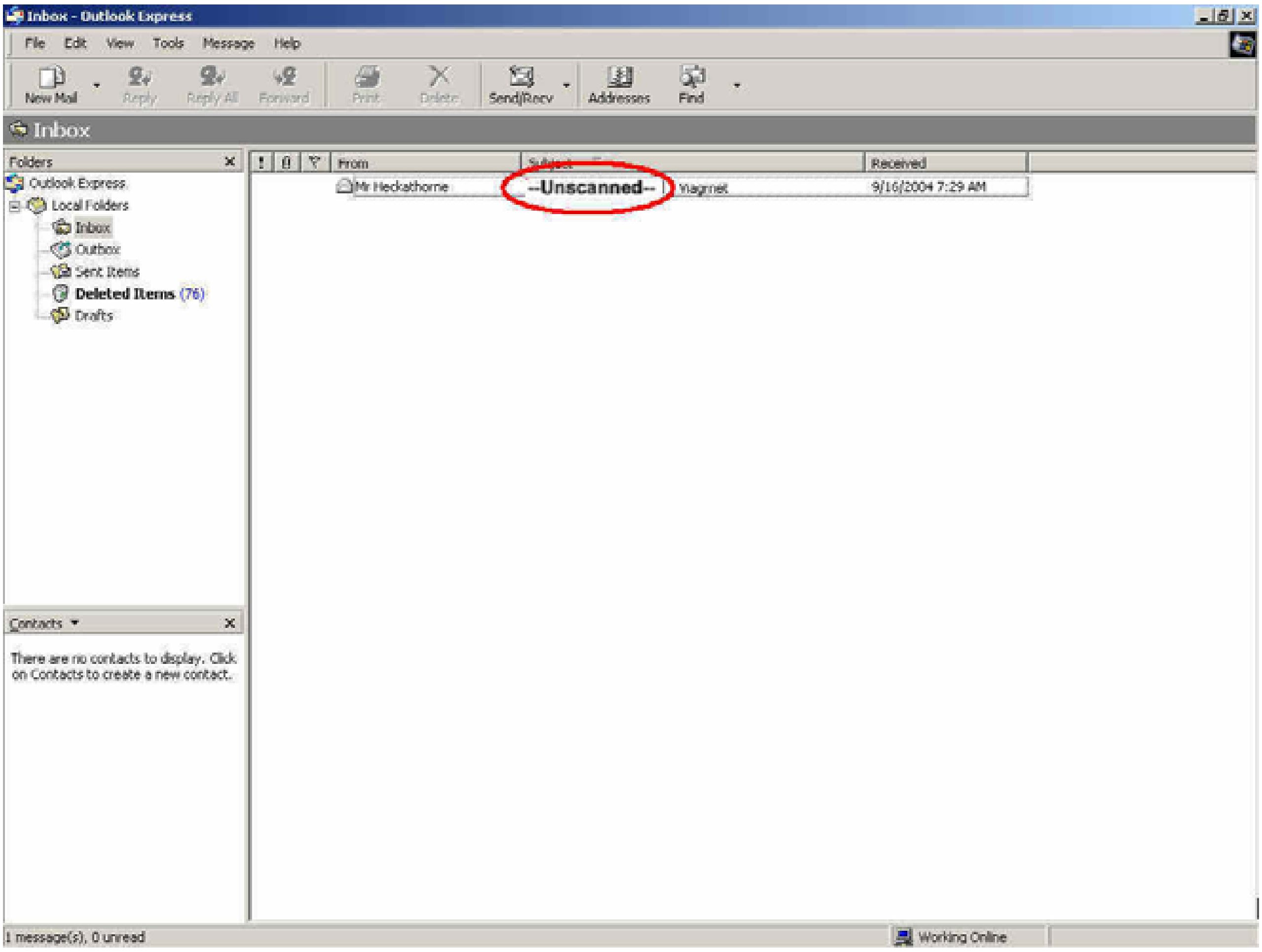
Scanned Mail Setting

The scanned mail size is less than 128 KBytes (10 - 512 KBytes)

Unscanned Mail Setting

□ Add the message to the subject line --Unscanned--

When receive unscanned mail, it will add the tag in front of the e-mail subject.



From	Subject	Received
Mr Heckathorne	--Unscanned-- Yiagnet	9/16/2004 7:29 AM

There are no contacts to display. Click on Contacts to create a new contact.

Mail Relay: After scanning the mails that sent to Internal Mail Server by **Anti-Spam** and **Anti-Virus** function of CS-500, then to setup the relevant setting in **Mail Relay** function. For the examples below you can understand more about how to configure your setting.

Example 1: To setup CS-500 as Gateway (Mail Server in DMZ, Transparent Mode)

Preparation:

WAN Port IP: 61.11.11.11

Mail Server IP: 61.11.11.12

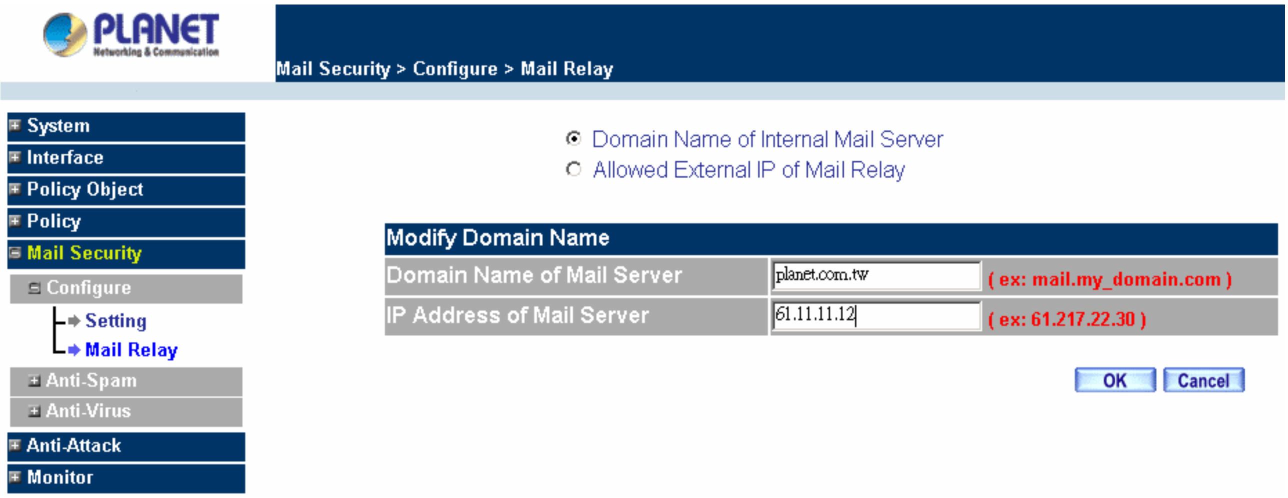
Map the DNS Domain Name that apply from ISP (planet.com.tw) to DNS Server IP (setup MX record is Mail Server IP)

When external sender sends mail to the recipient account of the planet.com.tw domain, add the following Mail Relay setting:

STEP 1. Add the following setting in **Mail Relay** function of **Configure**:

- Select **Domain Name of Internal Mail Server**
- **Domain Name of Mail Server:** Enter the Domain Name
- **IP Address of Mail Server:** Enter the IP address that Mail Server's domain name mapped to.

Mail Relay setting is complete. The external mails send to planet.com.tw that will be received by CS-500 and redirect to the mail server after filtering.



● Domain Name of Internal Mail Server
○ Allowed External IP of Mail Relay

Modify Domain Name		
Domain Name of Mail Server	planet.com.tw	(ex: mail.my_domain.com)
IP Address of Mail Server	61.11.11.12	(ex: 61.217.22.30)

Example 2: To setup CS-500 between the original Gateway and Mail Server (Mail Server in DMZ, Transparent Mode)

Preparation:

The Original Gateway's LAN Subnet: 172.16.1.0/16

WAN Port IP: 61.11.11.11

CS-500's WAN Port IP: 172.16.1.12

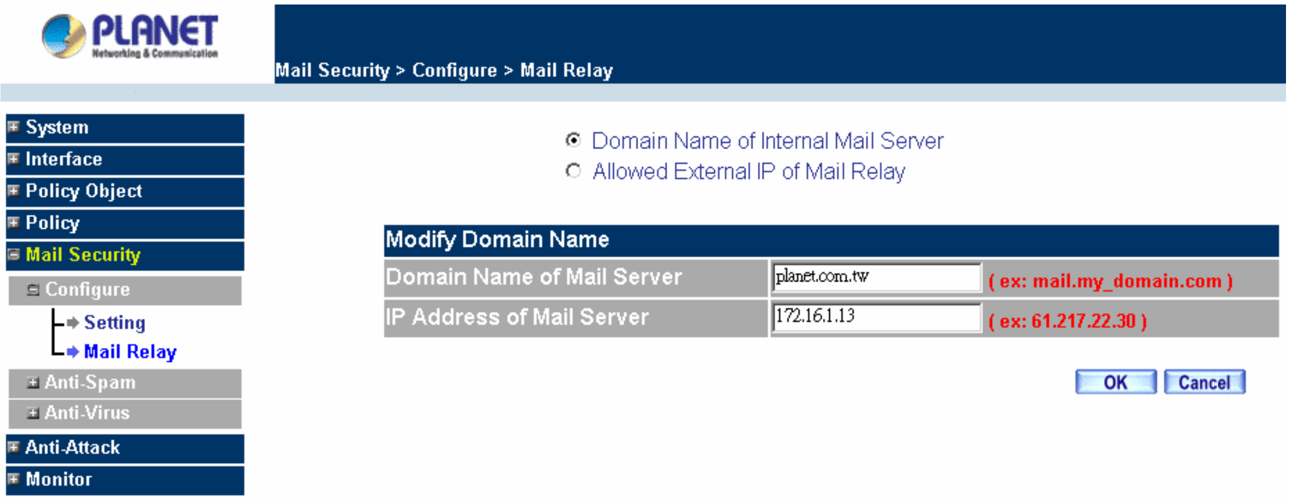
Mail Server IP: 172.16.1.13

Map the DNS Domain Name (planet.com.tw) to DNS Server IP (setup MX record is Mail Server IP)

When LAN (172.16.1.0/16) users send mail from the sender account of planet.com.tw mail server to the recipient account in external mail server, the configuration should need to add the following mail relay setting:

STEP 1. Add the first setting in **Mail Relay** function of **Configure**:

- Select **Domain Name of Internal Mail Server**
- **Domain Name of Mail Server:** Enter the Domain Name
- **IP Address of Mail Server:** Enter the IP address that Mail Server's domain name mapped to.

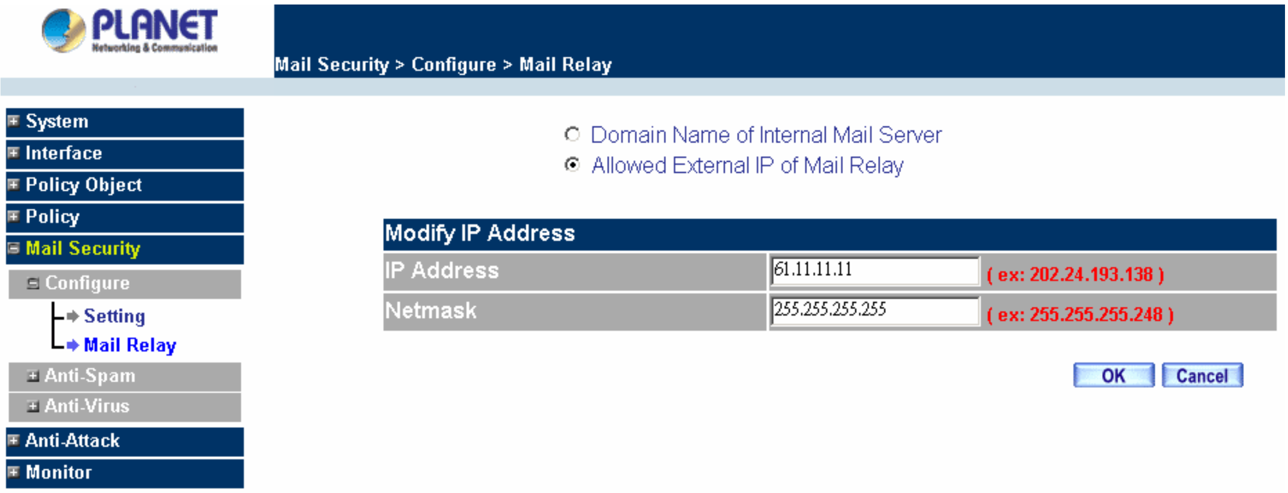


● Domain Name of Internal Mail Server
○ Allowed External IP of Mail Relay

Modify Domain Name		
Domain Name of Mail Server	planet.com.tw	(ex: mail.my_domain.com)
IP Address of Mail Server	172.16.1.13	(ex: 61.217.22.30)

STEP 2﹒Add the second setting in **Mail Relay** function of **Configure**:

- Select **Allowed External IP of Mail Relay**
- **IP Address:** Enter the IP Address of external sender
- Enter the **Netmask**
- Complete Mail Relay setting



○ Domain Name of Internal Mail Server
● Allowed External IP of Mail Relay

Modify IP Address		
IP Address	61.11.11.11	(ex: 202.24.193.138)
Netmask	255.255.255.255	(ex: 255.255.255.248)

Example 3: The Headquarters setup CS-500 as Gateway (Mail Server in DMZ, Transparent Mode) to make the Branch office's employees can send mails via Headquarters' Mail Server

Preparation:

WAN Port IP of CS-500: 61.11.11.11

Mail Server IP: 61.11.11.12

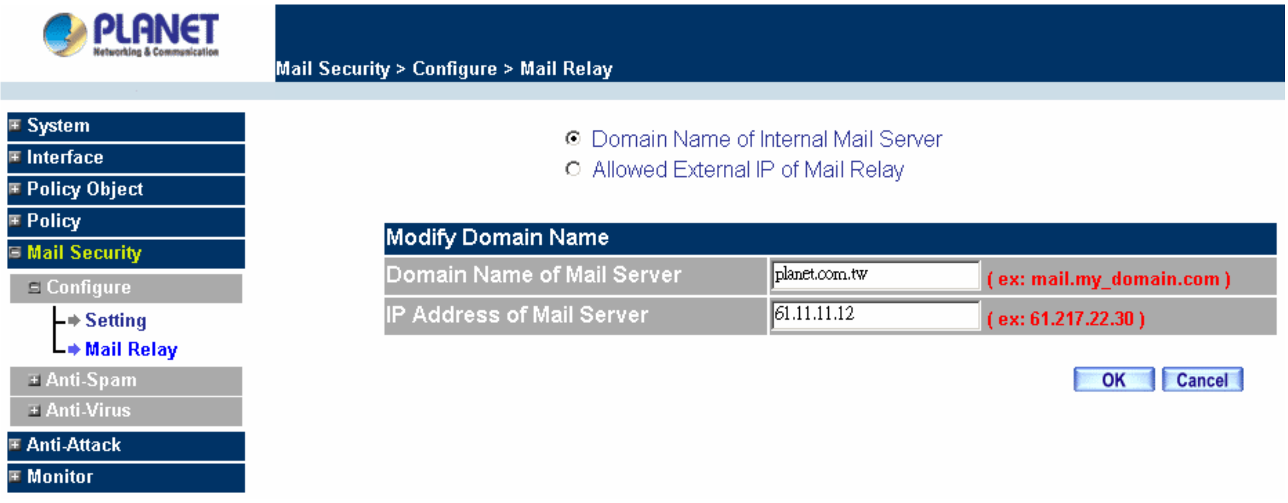
WAN Port IP of the Branch office's Firewall: 211.22.22.22

Map the DNS Domain Name (planet.com.tw) to DNS Server IP (setup MX record is Mail Server IP)

When the branch office's users send mail to the external mail server's recipient account from mail server's sender account of planet.com.tw, add the following Mail Relay setting:

STEP 1．Add the first setting in **Mail Relay** function of **Configure**:

- Select **Domain Name of Internal Mail Server**
- **Domain Name of Mail Server:** Enter the Domain Name
- **IP Address of Mail Server:** Enter the IP address that Mail Server's domain name mapped to.

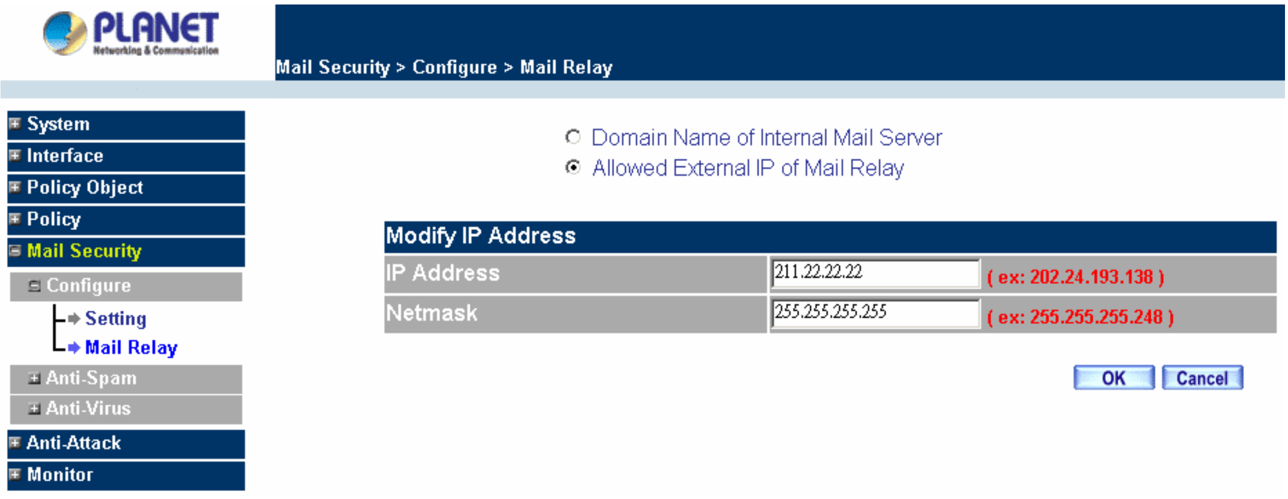


● Domain Name of Internal Mail Server
○ Allowed External IP of Mail Relay

Modify Domain Name		
Domain Name of Mail Server	planet.com.tw	(ex: mail.my_domain.com)
IP Address of Mail Server	61.11.11.12	(ex: 61.217.22.30)

STEP 2．Add the second setting in **Mail Relay** function of **Configure**:

- Select **Allowed External IP of Mail Relay**
- **IP Address:** Enter the IP Address of external sender
- Enter the **Netmask**
- Complete Mail Relay setting



○ Domain Name of Internal Mail Server
● Allowed External IP of Mail Relay

Modify IP Address		
IP Address	211.22.22.22	(ex: 202.24.193.138)
Netmask	255.255.255.255	(ex: 255.255.255.248)

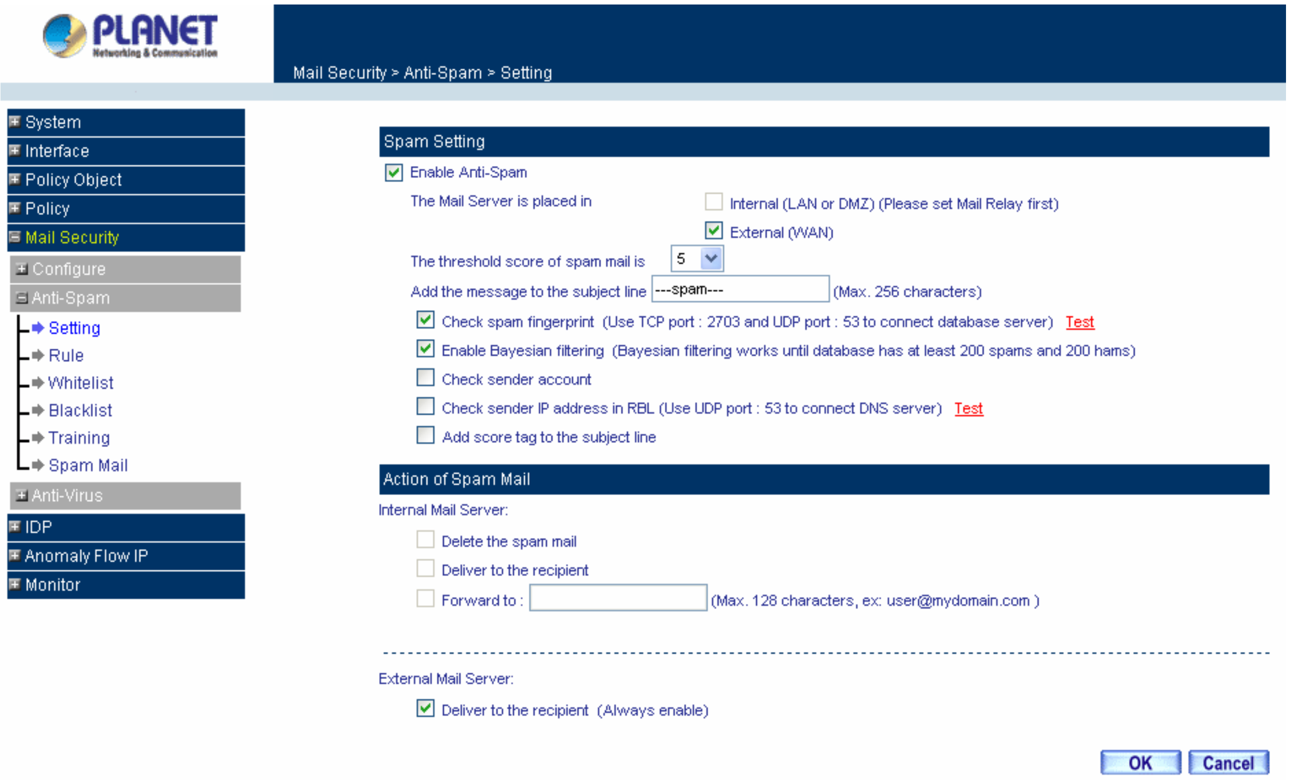
4.5.2 Anti-Spam

CS-500 can filter the e-mails that are going to send to the mail server of enterprise, in order to make sure the e-mail account that communicates with outside won't receive a mass advertisement or Spam mail. Meanwhile, it can reduce the burden of mail server. Also can prevent the users to pick up the message he/she needs from a mass of useless mails; or delete the needed mail mistakenly while deleting mails. It will raise the work efficiency of the employees and will not lose the important information of enterprise.

In this chapter, we will have the detailed illustration about **Anti-Spam:**

4.5.2.1 Setting

The Administrator can choose the inspection way of the mails, where the mail server is placed in Internal (LAN or DMZ) or External (WAN). CS-500 also can inspect all of the mails that are sent to the enterprise, and add a score tag or message to the subject line of Spam mail while it exceeds the standard. Meanwhile, it supports to check sender address in blacklist of anti-spam website to determine if it is spam mail or not.



Spam Setting

☑ Enable Anti-Spam

The Mail Server is placed in □ Internal (LAN or DMZ) (Please set Mail Relay first)

☑ External (WAN)

The threshold score of spam mail is 5

Add the message to the subject line ---spam--- (Max. 256 characters)

☑ Check spam fingerprint (Use TCP port : 2703 and UDP port : 53 to connect database server) Test

☑ Enable Bayesian filtering (Bayesian filtering works until database has at least 200 spams and 200 hams)

□ Check sender account

□ Check sender IP address in RBL (Use UDP port : 53 to connect DNS server) Test

□ Add score tag to the subject line

Action of Spam Mail

Internal Mail Server:

□ Delete the spam mail

□ Deliver to the recipient

□ Forward to : (Max. 128 characters, ex: user@mydomain.com)

External Mail Server:

☑ Deliver to the recipient (Always enable)

Definition:

Enable Anti-Spam: Select to enable Anti-Spam function.

The Mail Server is placed in Internal (LAN or DMZ) or External (WAN): Select to choose the location of the mail server.

The threshold score of spam mail is: CS-500 allows the Administrator to decide the threshold to be the standard of judging the spam mail.

Add the message to the subject line: If the mail has been judged to the spam mail, CS-500 will add a message in the mail's subject. You can configure the message you want, by default, it will be add "SPAM" in the subject.

Check spam fingerprint: Select to allow CS-500 checking spam mail with Fingerprint system.

Enable Bayesian filtering: Except to select fingerprinter system to distinguish spam mail, you also can select Bayesian filtering system to scan spam mail.

Check sender account: Select to allow CS-500 checking sender's account when it receives the mail, if the sender's account is faked, CS-500 will treat the mail as the spam.

Check sender IP address in RBL (Realtime Blackhole List): Select this function to allow CS-500 checking mail with RBL list.

Add score tag to the subject line: If select this function, all received mail will be added a score tag in the mail subject.

Action of Spam Mail: When CS-500 filters the spam mail, there are three kinds of actions for Internal Mail Server and one action for External Mail server to arrange the spam mail:

Delete the spam mail: If select this option, the spam mail will be deleted without any notification.

Deliver to the recipient: Pass the mail to the recipient, and add a "SPAM" in the mail subject. This function is available for Internal and External Mail Server.

Forward to: You can configure CS-500 to forward spam mail to a specific mail account; it will be easily to manage the spam mail.

Configure an Anti- Spam setting

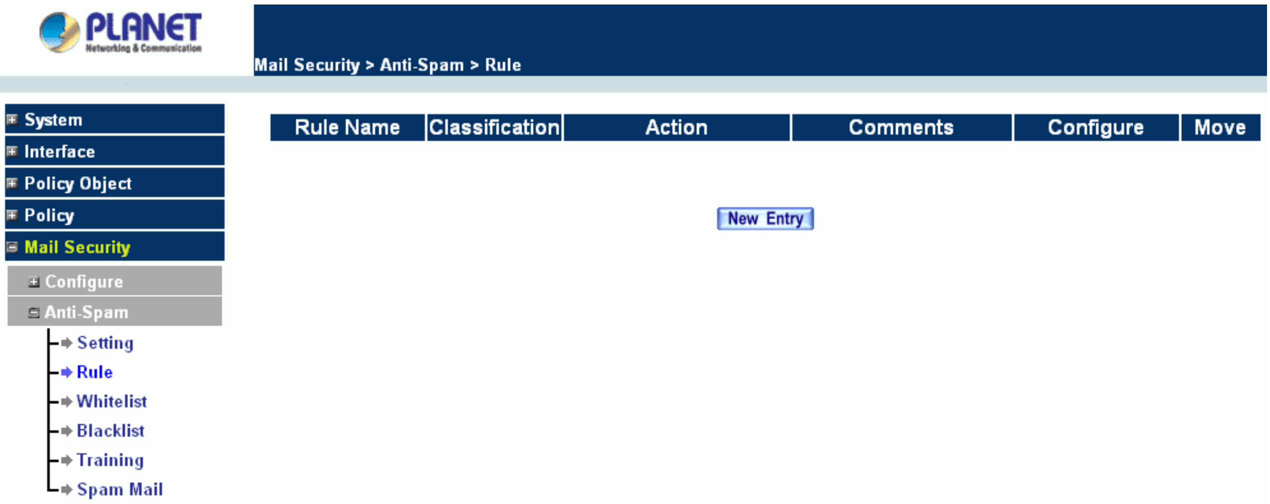
After setup the relevant settings in **Mail Relay** function of **Configure**, add the following settings in this function:

1. The Mail Server is placed in **Internal (LAN or DMZ)**
2. **The threshold score**: Enter 5
3. **Add the message to the subject line**: Enter ---spam---
4. Select **Add score tag to the subject line**
5. Select **Deliver to the recipient**
6. Click **OK**.

4.5.2.2 Rule

The Content Security Gateway's Administrator may use the rule setting to classify the spam mail based on a certain condition. The rule also can allow CS-500 to record the mail type by auto-learning system to judge the spam mail.

Click on **Mail Security** in the menu bar, then click on **Rule** below the **Anti-Spam** menu. The Rule window will appear.



Below is the information needed for setting up the **Rule**:

- **Rule Name:** The name of the custom spam mail determination rule.
- **Comments:** To explain the meaning of the custom rule.
- **Combination:**

  And: It must be fit in with all of the custom mail rules that would be considered as spam mail or ham mail.

  Or: Only be fit in with one of the custom mail rule that would be considered as spam mail or ham mail.
- **Classification:**

  Spam: It will classify the mails that correspond to the rule as spam mail.

  Ham (Non-Spam): It will classify the mails that correspond to the rule as ham mail.
- **Action:** This function will be available only when **Classification** is set as **Spam**. You can choose the action to **Delete spam mail**, **Deliver to the recipient**, or **Forward to** another mail account.
- **Auto-Training:** If **Classification** is set as **Spam** and enable this function, the mails that correspond to this rule will be trained to identify as spam mail; or if **Classification** is set as **Ham (Non-Spam)** and enable this function, the mails correspond to this rule will be trained to identify as ham (non-spam) mail according to the setting in Training function
- **Item:** The items use to judge the spam mail according to **Header**, **Body** and **Size** of the mail. The packet Header includes: **Received**, **Envelope-To**, **Form**, **To**, **Cc**, **Bcc**, **Subject**, **Sender**, **Reply-To**, **Errors-To**, **Message-ID**, and **Date**.
- **Condition:**

  Item set to Header or Body: The available conditions are: **Contains**, **Does Not Contain**, **Is Equal To**, **Is Not Equal To**, **Starts With**, **Ends With**, **Exist** and **Does Not Exist**.

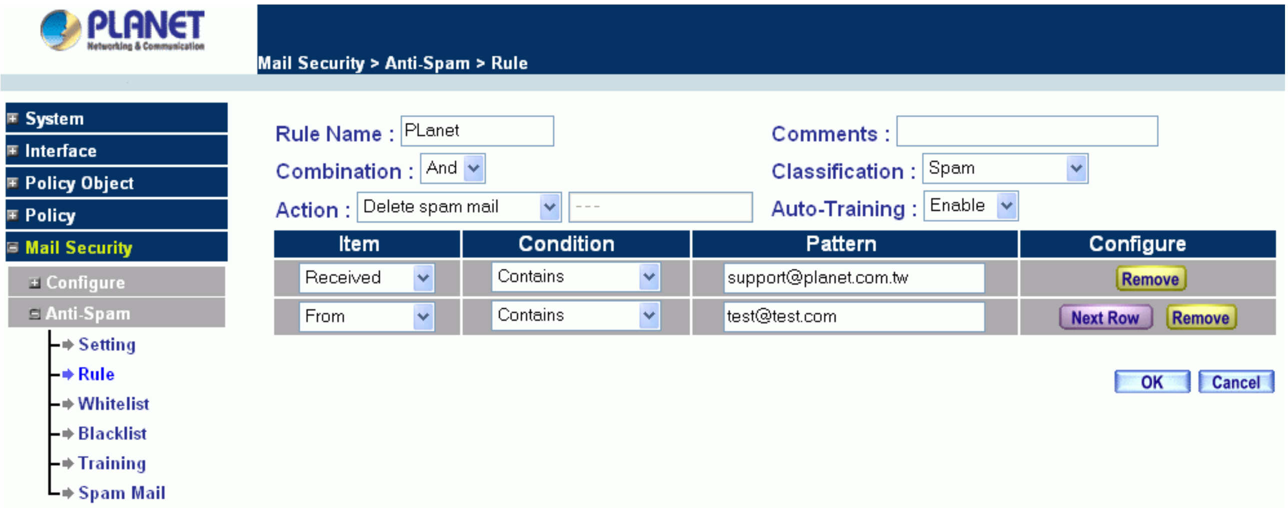
  Item set to Size: The available conditions are: **More Than**, **Is Equal To**, **Is Not Equal To** and **Less Than**.
- **Pattern:** Enter the relevant value in **Item** and **Condition** field. For example: **From** Item and use **Contains** Condition, and enter "josh" as a characteristics. When the sender and receiver's mail account has "josh" inside and then it will be considered as spam mail or ham mail

Adding a new Rule

Step 1: Click on the **New Entry** button and the **Rule** window will appear.

Step 2: Fill in the appropriate settings for the related information..

Step 3: Click **OK** to save the policy or **Cancel** to cancel.



Rule Name : PLanet
Comments :
Combination : And
Classification : Spam
Action : Delete spam mail ---
Auto-Training : Enable

Item	Condition	Pattern	Configure
Received	Contains	support@planet.com.tw	Remove
From	Contains	test@test.com	Next Row Remove

Modifying a Rule

Step 1: In the **Rule** window, find the policy to be modified and click the corresponding **Modify** option in the **Configure** field.

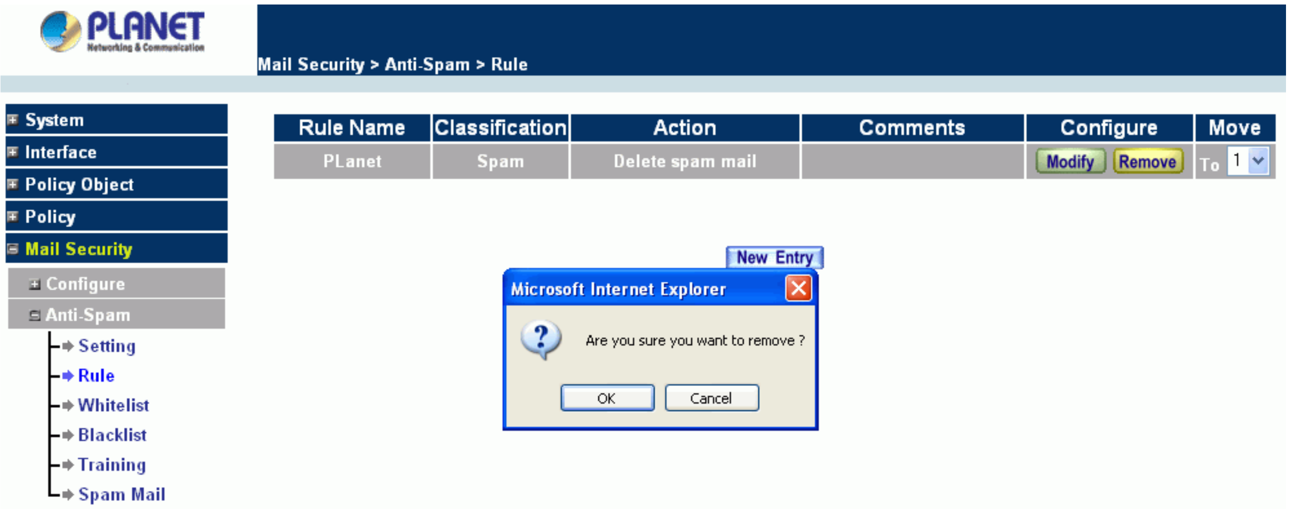
Step 2: Make the necessary changes needed.

Step 3: Click **OK** to save changes or click on **Cancel** to cancel modifications.

Removing a Rule

Step 1: In the **Rule** window, find the policy to be removed and click the corresponding **Remove** option in the **Configure** field.

Step 2: A confirmation pop-up box will appear, click **OK** to remove the Host Table or click **Cancel**.



Rule Name	Classification	Action	Comments	Configure	Move
PLanet	Spam	Delete spam mail		Modify Remove	To 1

Are you sure you want to remove ?

4.5.2.3 Whitelist

To determine the mail comes from specific mail address that can send to the recipient without being restricted.

Below is the information needed for setting up the **Whitelist**

- **Whitelist:** Specify the key word or with wildcard for the Whitelist field..
- **Direction:**

  From: To judge the sending address of the mail.

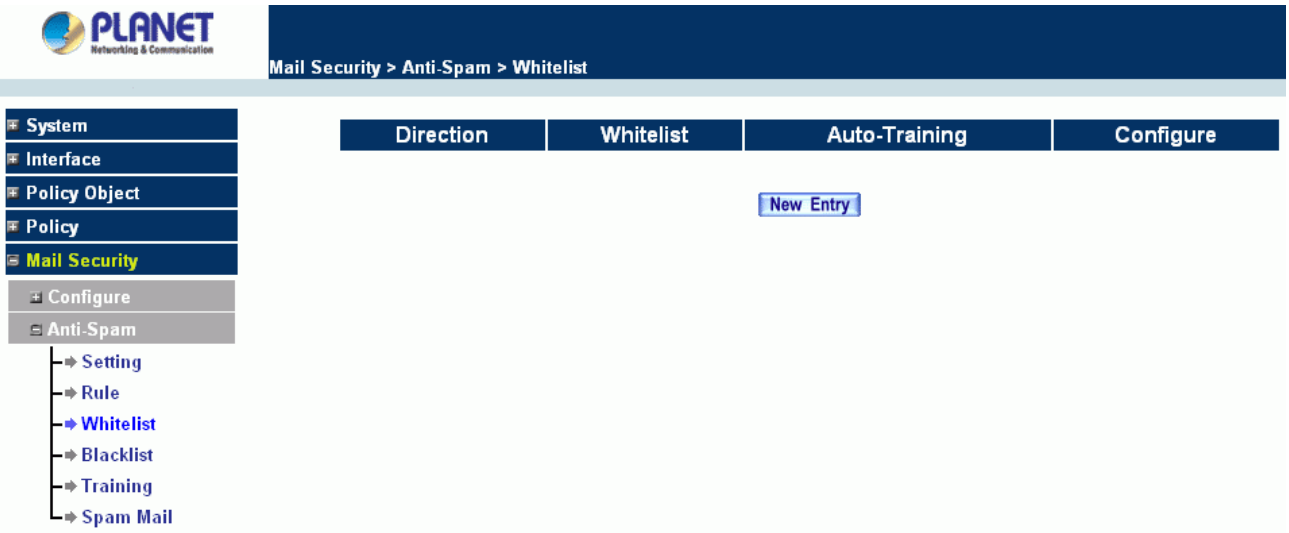
  To: To judge the receiving address of the mail.
- **Auto-Training:** Select enable to allow Auto-Training system updating the CS-500's database.

Adding a new Whitelist

Step 1: Click on the **New Entry** button and the **Whitelist** window will appear.

Step 2: Fill in the appropriate settings for the related information..

Step 3: Click **OK** to save the policy or **Cancel** to cancel.

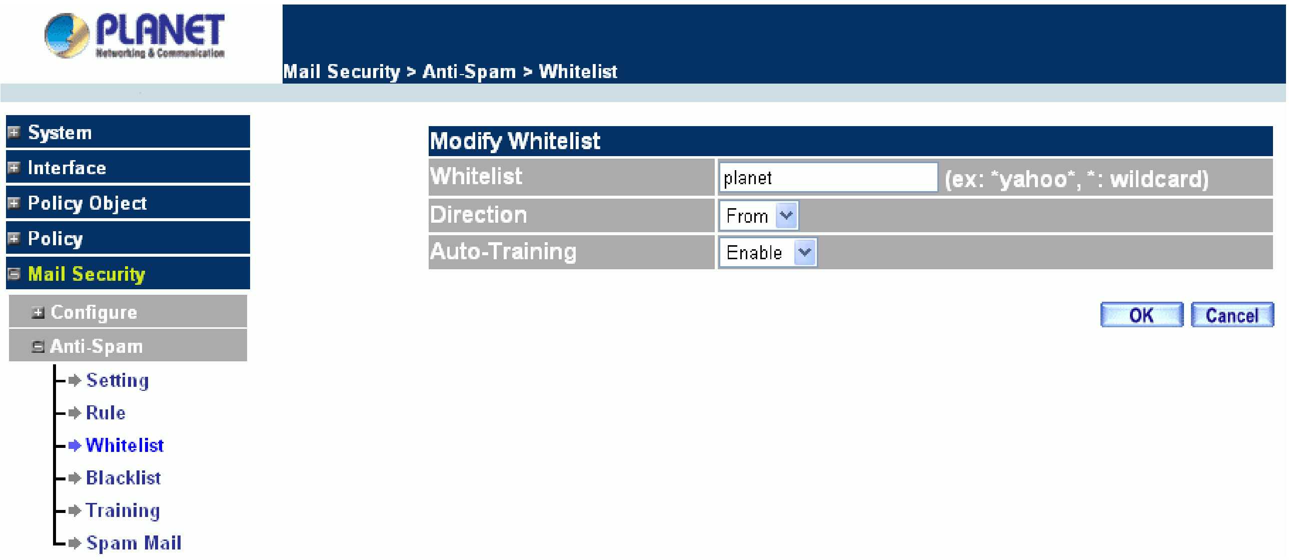


Modifying a Whitelist

Step 1: In the **Whitelist** window, find the policy to be modified and click the corresponding **Modify** option in the **Configure** field.

Step 2: Make the necessary changes needed.

Step 3: Click **OK** to save changes or click on **Cancel** to cancel modifications.

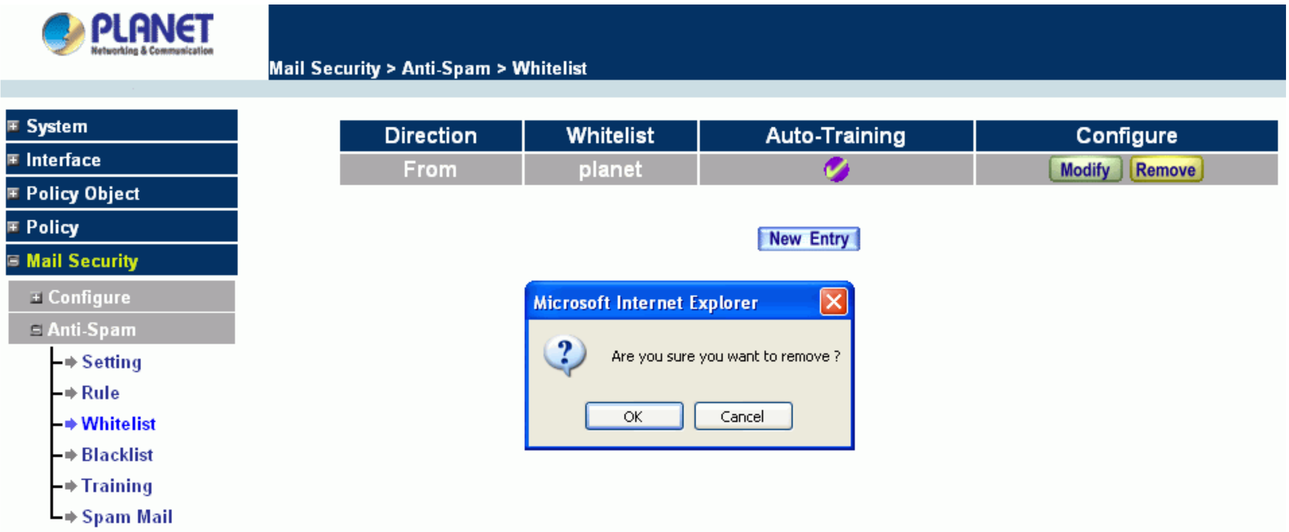


Modify Whitelist	
Whitelist	planet (ex: *yahoo*, *: wildcard)
Direction	From
Auto-Training	Enable

Removing a Whitelist

Step 1: In the **Rule** window, find the policy to be removed and click the corresponding **Remove** option in the **Configure** field.

Step 2: A confirmation pop-up box will appear, click **OK** to remove the Host Table or click **Cancel**.



Direction	Whitelist	Auto-Training	Configure
From	planet	✓	Modify Remove

Are you sure you want to remove ?

4.5.2.4 Blacklist

To determine the mail comes from specific mail address that will be filtered or restricted.

Below is the information needed for setting up the **Blacklist**

- **Blacklist:** Specify the key word or with wildcard for the Blacklist field.
- **Direction:**

  From: To judge the sending address of the mail.

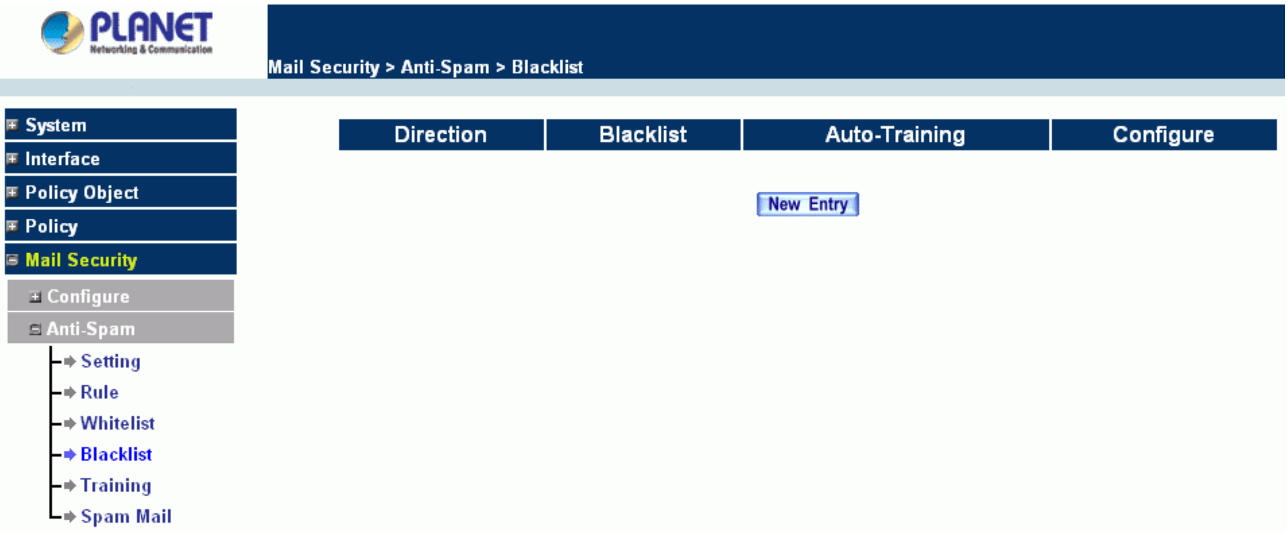
  To: To judge the receiving address of the mail.
- **Auto-Training:** Select enable to allow Auto-Training system updating the CS-500's database.

Adding a new Blacklist

Step 1: Click on the **New Entry** button and the **Blacklist** window will appear.

Step 2: Fill in the appropriate settings for the related information..

Step 3: Click **OK** to save the policy or **Cancel** to cancel.



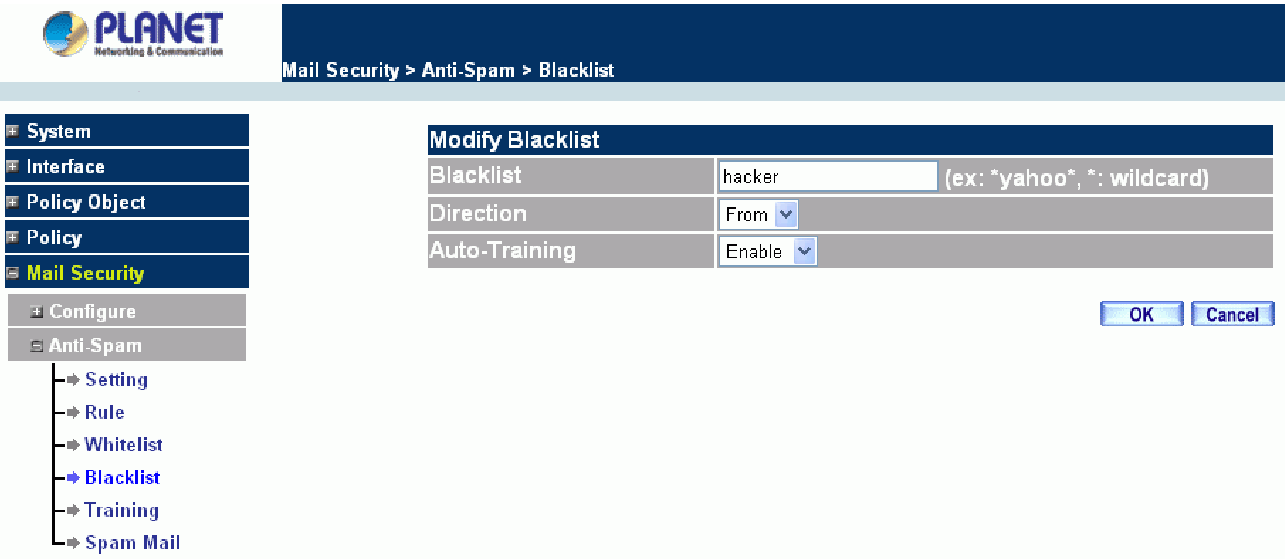
Direction	Blacklist	Auto-Training	Configure

Modifying a Blacklist

Step 1: In the **Blacklist** window, find the policy to be modified and click the corresponding **Modify** option in the **Configure** field.

Step 2: Make the necessary changes needed.

Step 3: Click **OK** to save changes or click on **Cancel** to cancel modifications.



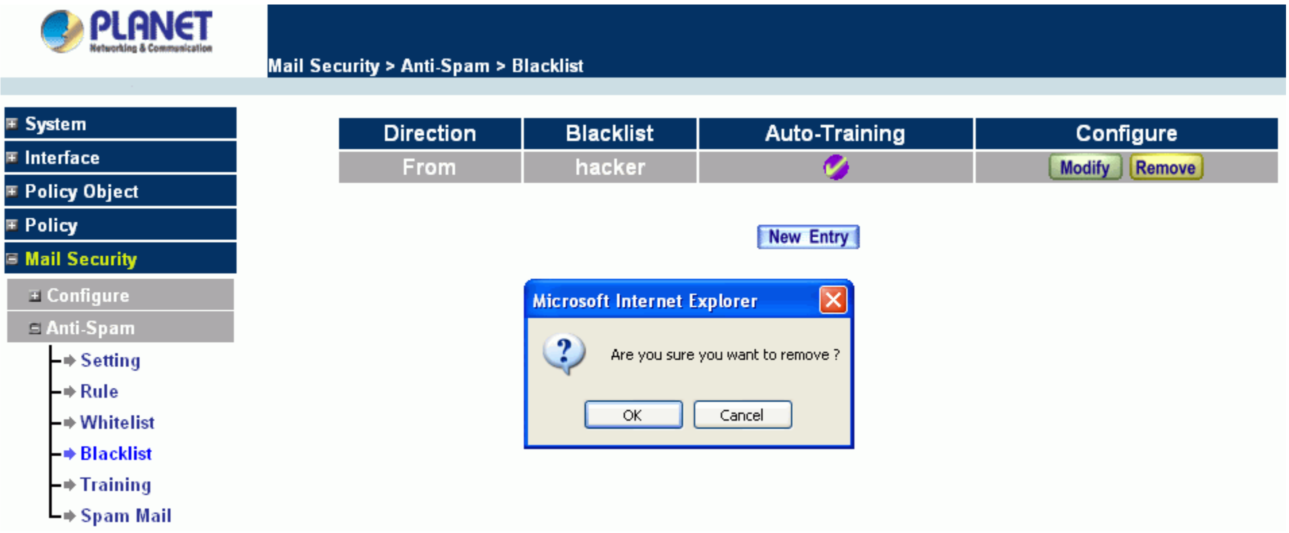
Modify Blacklist

Blacklist	hacker (ex: *yahoo*, *: wildcard)
Direction	From
Auto-Training	Enable

Removing a Blacklist

Step 1: In the **Blacklist** window, find the policy to be removed and click the corresponding **Remove** option in the **Configure** field.

Step 2: A confirmation pop-up box will appear, click **OK** to remove the Host Table or click **Cancel**.



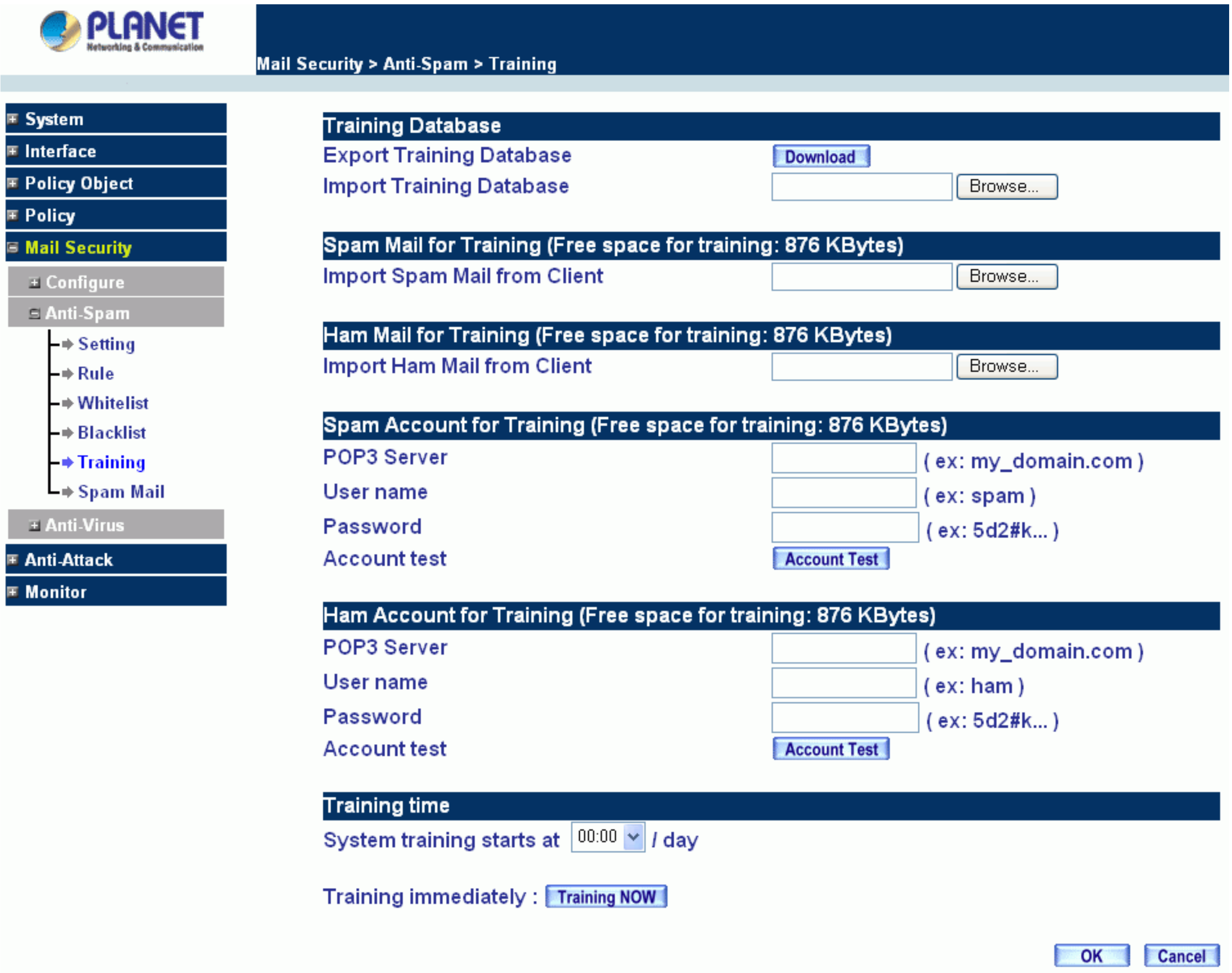
Direction	Blacklist	Auto-Training	Configure
From	hacker	✓	Modify Remove

Are you sure you want to remove ?

4.5.2.5 Training

CS-500 provides a training system to improve the identify rate of spam, the database can be updated by manually or from the rule setting. Below is the information needed for setting up the **Training**.

- **Training Database:** The System Manager can Import or Export Training Database here.
- **Spam Mail for Training:** The System Manager can import the file which is not determined as spam mail here. To raise the judgment rate of spam mail after the CS-500 learning the file.
- **Ham Mail for Training:** The System Manager can import the file which is determined as spam mail here. To raise the judgment rate of ham mail after the CS-500 learning the file
- **Spam Account for Training:** You can specify a mail account in your mail server, and redirect all the Spam mail to this account. When the related configuration is set, such as **POP3 server**, **User name** and **Password**, CS-500 will search the Spam mail in this account and update the Spam type to the database in a regular time.
- **Ham Account for Training:** You can specify a mail account in your mail server, and redirect all the Ham mail to this account. When the related configuration is set, such as **POP3 server**, **User name** and **Password**, CS-500 will search the Ham mail in this account and update the Ham type to the database in a regular time.
- **Training Time:** The System Manager can set the training time for CS-500 to learn the import file each day here.



Training Database

Export Training Database [Download]

Import Training Database [Browse...]

Spam Mail for Training (Free space for training: 876 KBytes)

Import Spam Mail from Client [Browse...]

Ham Mail for Training (Free space for training: 876 KBytes)

Import Ham Mail from Client [Browse...]

Spam Account for Training (Free space for training: 876 KBytes)

POP3 Server (ex: my_domain.com)

User name (ex: spam)

Password (ex: 5d2#k...)

Account test [Account Test]

Ham Account for Training (Free space for training: 876 KBytes)

POP3 Server (ex: my_domain.com)

User name (ex: ham)

Password (ex: 5d2#k...)

Account test [Account Test]

Training time

System training starts at 00:00 / day

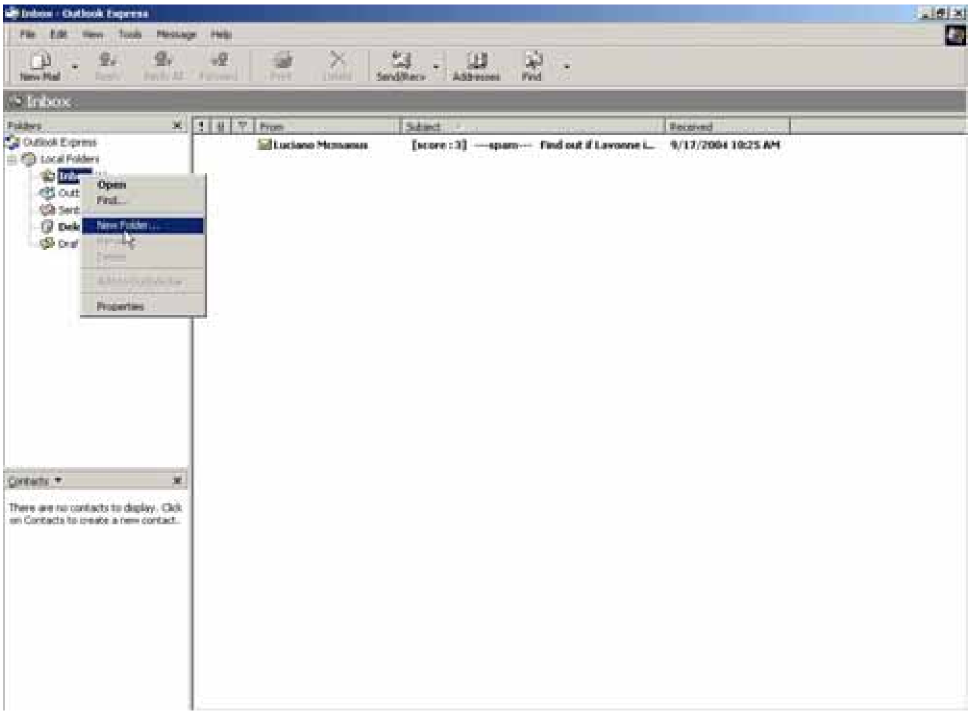
Training immediately : [Training NOW]

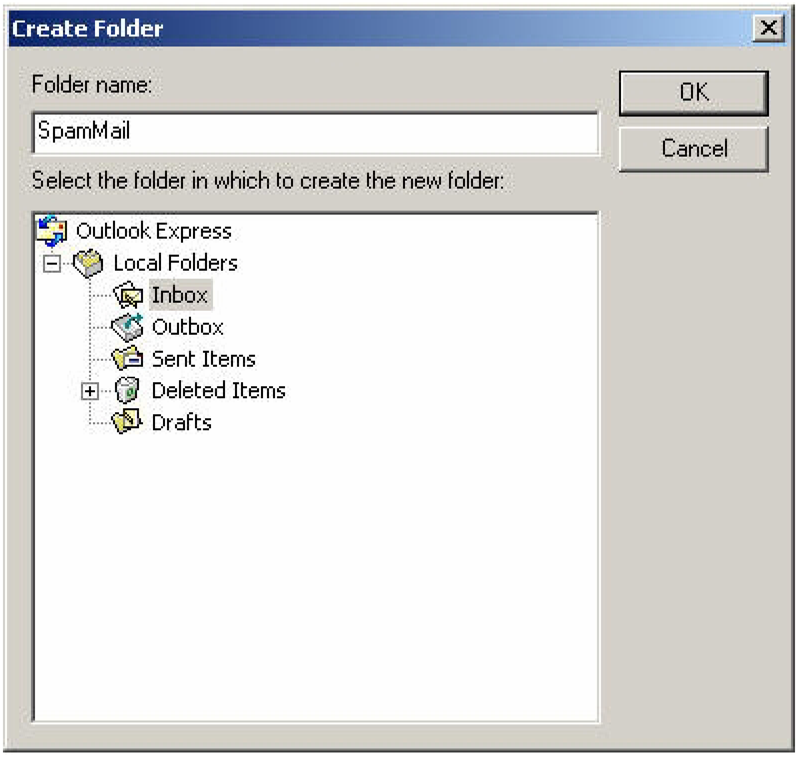
[OK] [Cancel]

Example: How to train mail into CS-500

STEP 1. Create a new folder SpamMail in **Outlook Express**:

- Press the right key of the mouse and select **New Folder**.
- In **Create Folder** WebUI and enter the Folder's Name as SpamMail, and then click on OK.

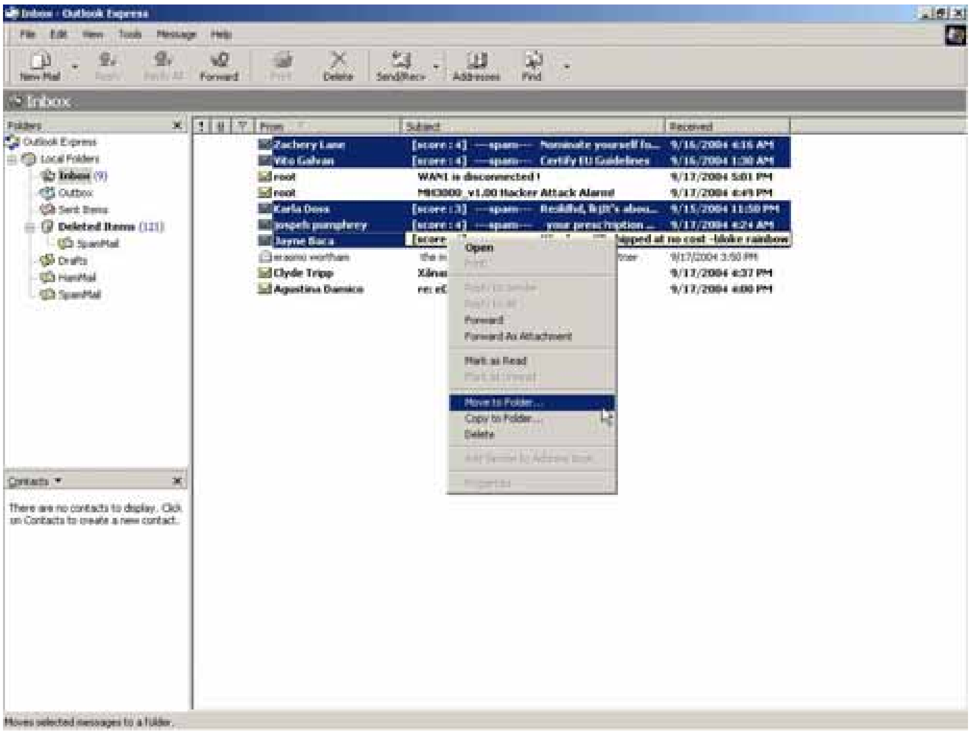




Folder name: SpamMail

STEP 2．In **Inbox-Outlook Express**, move spam mail to **SpamMail** Folder:

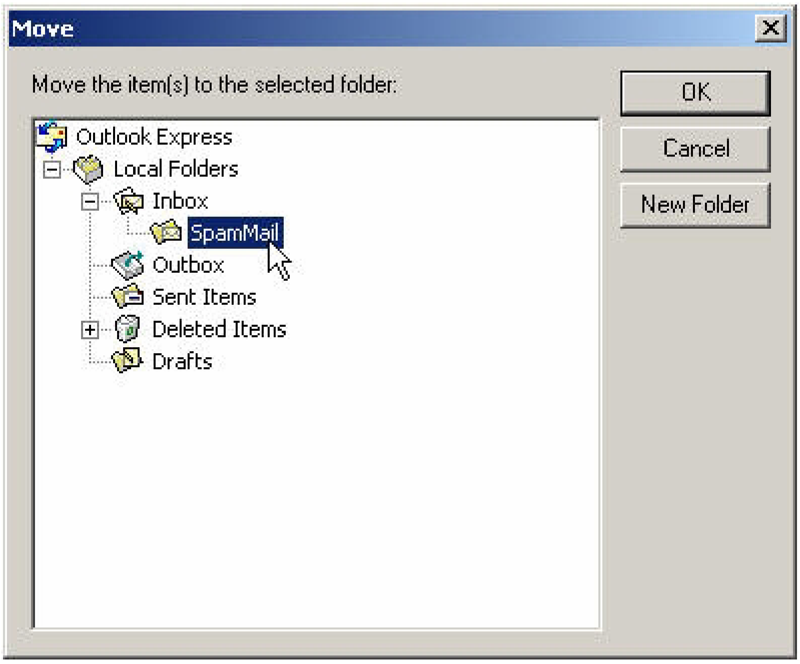
- In Inbox, select all of the spam mails that do not judge correctly and press the right key of the mouse and move to the folder.
- In **Move** WebUI, select **SpamMail** Folder and click **OK.**



From	Subject	Received
Zachery Lane	[score : 4] ---spam--- Nominate yourself fo...	9/16/2004 4:16 AM
Vito Galvan	[score : 4] ---spam--- Certify EU Guidelines	9/16/2004 1:30 AM
root	WAN1 is disconnected !	9/17/2004 5:01 PM
root	MH3000_v1.00 Hacker Attack Alarm!	9/17/2004 4:49 PM
Karla Doss	[score : 3] ---spam--- Rediolful, lt;jit's abou...	9/15/2004 11:50 PM
joseph pumphrey	[score : 4] ---spam--- your prescription ...	9/17/2004 4:24 AM
Jayne Baca	[score ... hipped at no cost -blake rainbow	
erasmo worthan	the ...	9/17/2004 3:50 PM
Clyde Tripp	Xäna...	9/17/2004 4:37 PM
Agustina Damico	re: e...	9/17/2004 4:00 PM

There are no contacts to display. Click on Contacts to create a new contact.

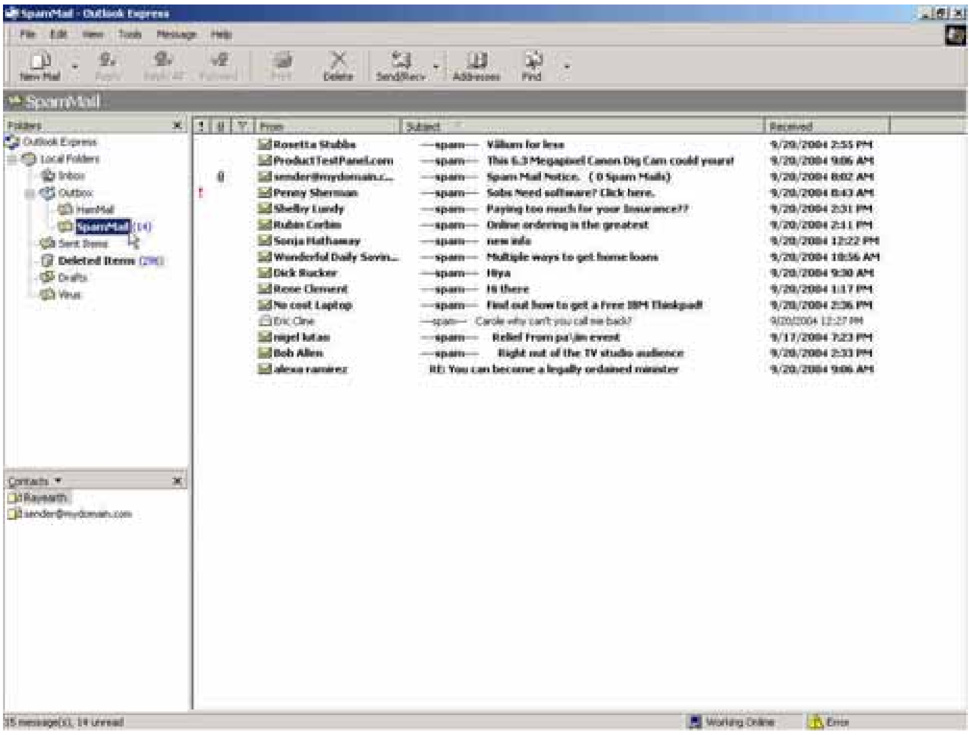
Moves selected messages to a folder.



Move the item(s) to the selected folder:

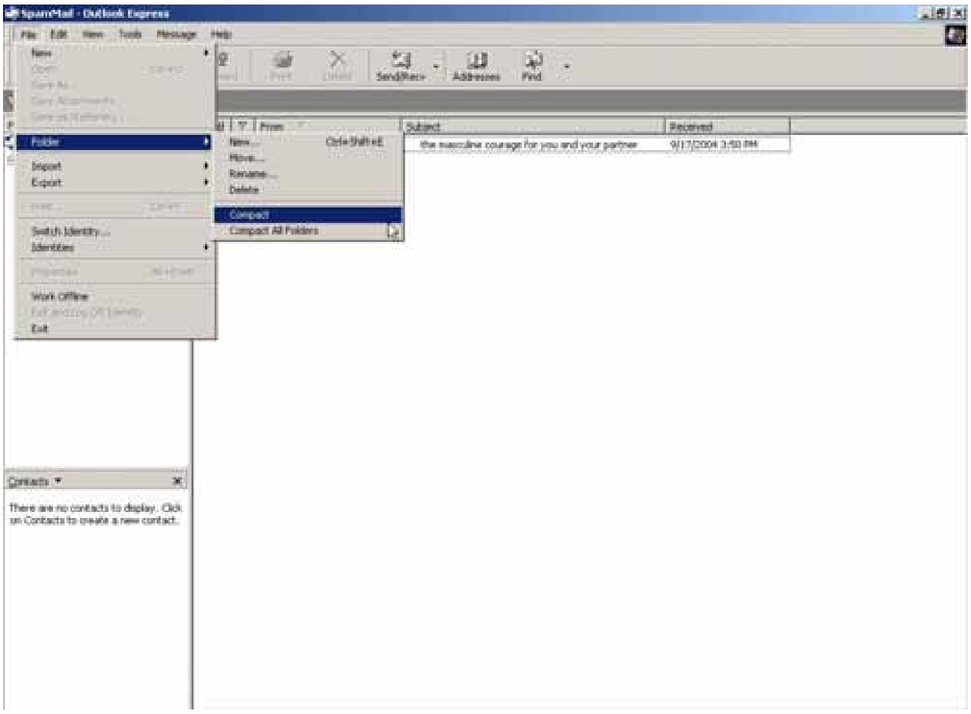
STEP 3. Compress the SpamMail Folder in **Outlook Express** to shorten the data and upload to CS-500 for training:

- Select **SpamMail** Folder
- Select **Compact** function in selection of the folder



!	0	▽	From	Subject	Received
			Rosetta Stubbs	—spam— Valium for less	9/20/2004 2:55 PM
			ProductTestPanel.com	—spam— This 6.3 Megapixel Canon Dig Cam could yours!	9/20/2004 9:06 AM
	0		sender@mydomain.c...	—spam— Spam Mail Notice. (0 Spam Mails)	9/20/2004 8:02 AM
!			Penny Sherman	—spam— Sobs Need software? Click here.	9/20/2004 8:43 AM
			Shelby Lundy	—spam— Paying too much for your Insurance??	9/20/2004 2:31 PM
			Rubin Corbin	—spam— Online ordering is the greatest	9/20/2004 2:11 PM
			Sonja Hathaway	—spam— new info	9/20/2004 12:22 PM
			Wonderful Daily Savin...	—spam— Multiple ways to get home loans	9/20/2004 10:56 AM
			Dick Rucker	—spam— Hiya	9/20/2004 9:30 AM
			Rene Clement	—spam— Hi there	9/20/2004 1:17 PM
			No cost Laptop	—spam— Find out how to get a Free IBM Thinkpad!	9/20/2004 2:36 PM
			Eric Cline	—spam— Carole why can't you call me back?	9/20/2004 12:27 PM
			nigel lutas	—spam— Relief From pa\in event	9/17/2004 7:23 PM
			Bob Allen	—spam— Right out of the TV studio audience	9/20/2004 2:33 PM
			alexa ramirez	RE: You can become a legally ordained minister	9/20/2004 9:06 AM

15 message(s), 14 unread

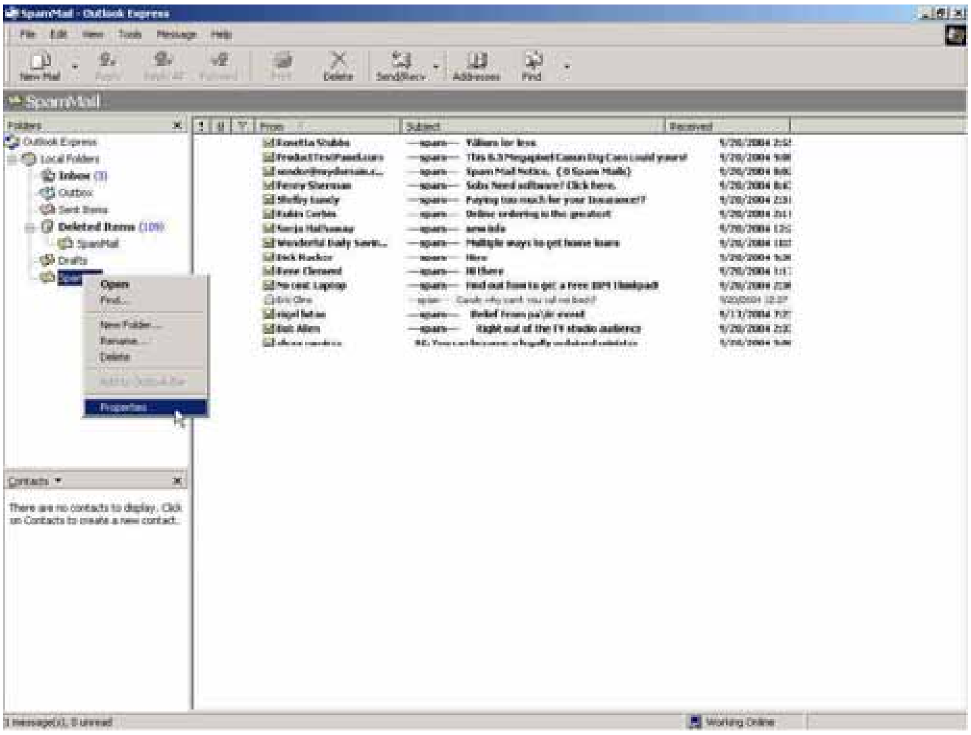


the masculine courage for you and your partner 9/17/2004 3:50 PM

There are no contacts to display. Click on Contacts to create a new contact.

STEP 4 . To copy the route of SpamMail File in **Outlook Express** to convenient to upload the training to CS-500:

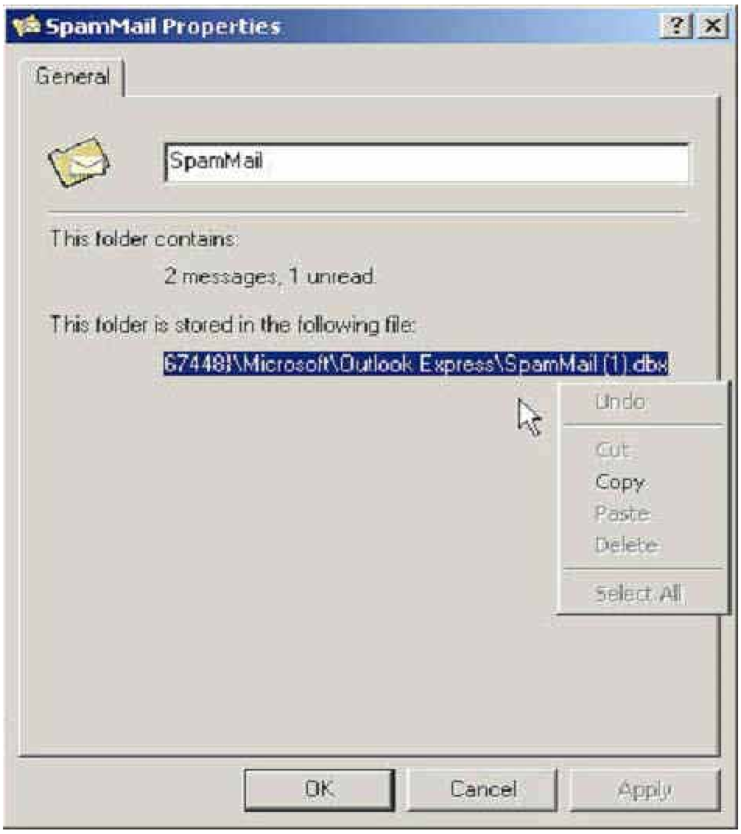
- Press the right key of the mouse in SpamMail file and select **Properties** function.
- Copy the file address in **SpamMail Properties** WebUI.



From	Subject	Received
Rosetta Stubbs	—spam— Valium for less.	9/20/2004 2:5
ProductTestPanel.com	—spam— This 6.3 Megapixel Canon Digi Cam could yours!	9/20/2004 9:0
sender@mydomain.c...	—spam— Spam Mail Notice. (0 Spam Mails)	9/20/2004 8:0
Penny Sherman	—spam— Subs Need software? Click here.	9/20/2004 8:
Shelby Lundy	—spam— Paying too much for your Insurance??	9/20/2004 2:3
Robin Corbin	—spam— Online ordering is the greatest	9/20/2004 2:1
Sonja Halloway	—spam— new info	9/20/2004 12:
Wonderful Daily Savin...	—spam— Multiple ways to get home loans	9/20/2004 10:
Dick Hacker	—spam— Here	9/20/2004 9:
Rene Clement	—spam— Hi there	9/20/2004 11:
No cost Laptop	—spam— Find out how to get a free IBM thinkpad	9/20/2004 2:
Eric Cline	—spam— Carole why can't you call me back?	9/20/2004 12:37
nigel fulton	—spam— Relief from pa\in event	9/13/2004 7:
Bob Allen	—spam— Right out of the TV studio audience	9/20/2004 2:
[illegible]	RE: You can become a legally ordained minister	9/20/2004 9:

There are no contacts to display. Click on Contacts to create a new contact.

1 message(s), 0 unread



SpamMail

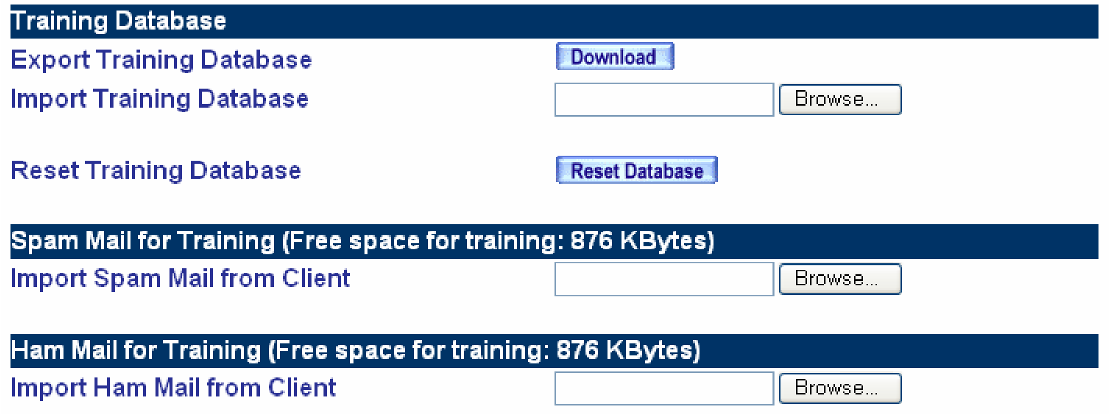
This folder contains:

2 messages, 1 unread

This folder is stored in the following file:

67448}\Microsoft\Outlook Express\SpamMail (1).dbx

STEP 5 . Paste the route of copied from SpamMail file to the **Spam Mail for Training** field in **Training** function of **Anti-Spam**. And press **OK** to deliver this file to CS-500 instantly and to learn the uploaded mail file as spam mail in the appointed time.



Training Database

Export Training Database	Download
Import Training Database	Browse...
Reset Training Database	Reset Database

Spam Mail for Training (Free space for training: 876 KBytes)

Import Spam Mail from Client	Browse...

Ham Mail for Training (Free space for training: 876 KBytes)

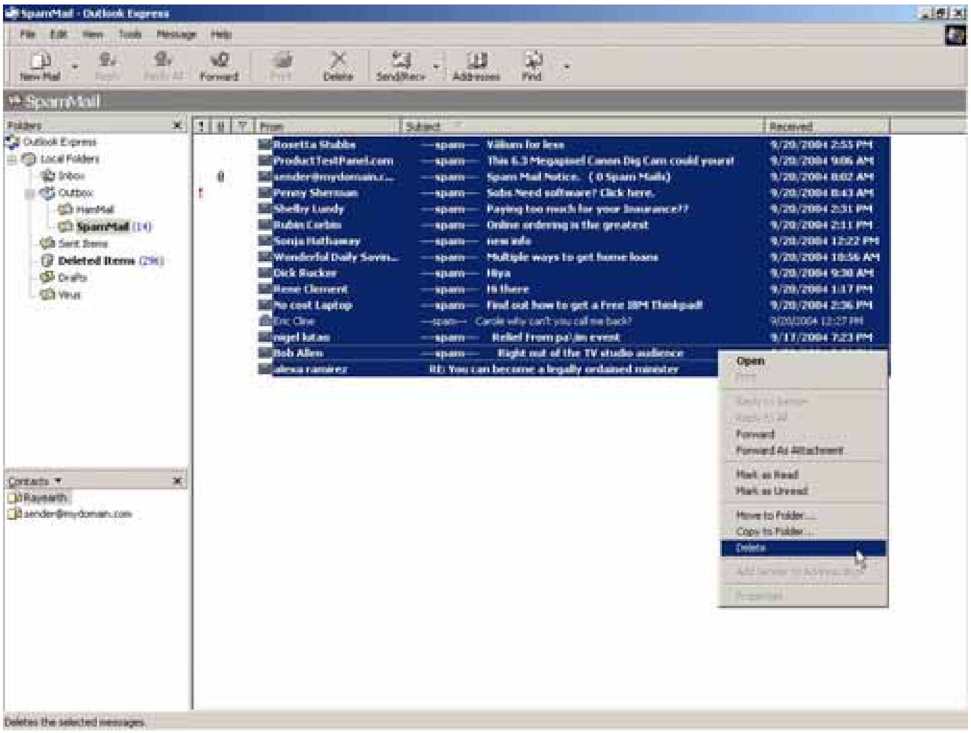
Import Ham Mail from Client	Browse...

Note:

1. **The training file that uploads to CS-500 can be any data file and not restricted in its sub-name, but the file must be ACSII form.**
2. **When the training file of CS-500 is Microsoft Office Outlook exporting file [.pst], it has to close Microsoft Office Outlook first to start Importing.**

STEP 6 . Remove all of the mails in **SpamMail** File in **Outlook Express** so that new mails can be compressed and upload to CS-500 to training directly next time.

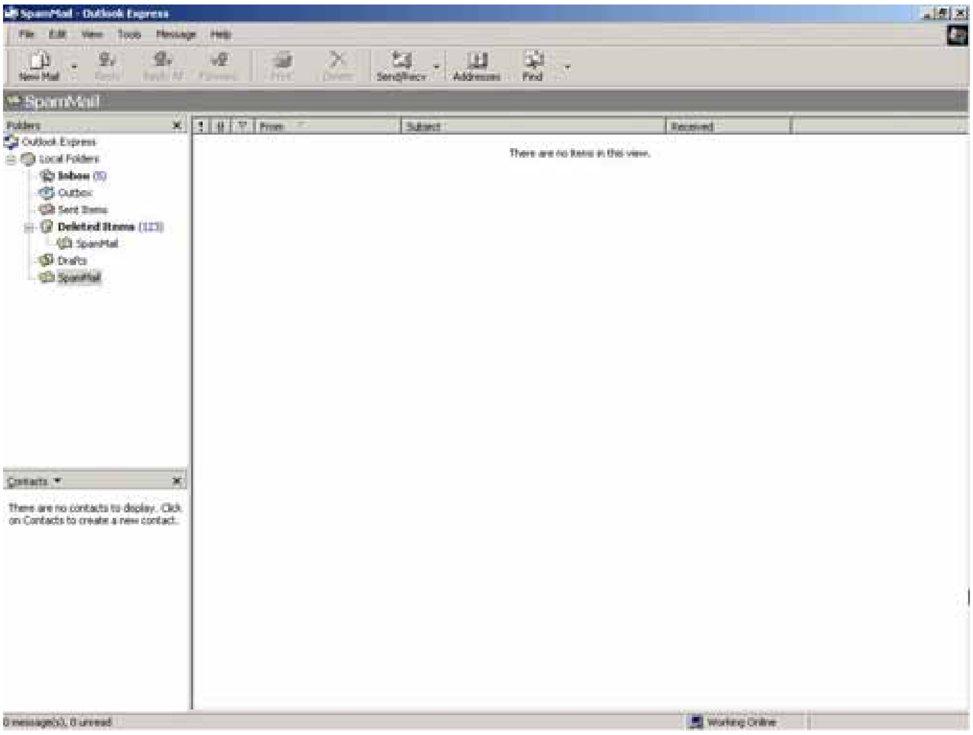
- Select all of the mails in **SpamMail** File and press the right key of the mouse to select **Delete** function.
- Make sure that all of the mails in SpamMail file had been deleted completely.



SpamMail - Outlook Express

From	Subject	Received
Rosetta Stubbs	—spam— Valium for less	9/20/2004 2:55 PM
ProductTestPanel.com	—spam— This 6.3 Megapixel Canon Dig Cam could yours!	9/20/2004 9:06 AM
sender@mydomain.c...	—spam— Spam Mail Notice. (0 Spam Mails)	9/20/2004 8:02 AM
Penny Sherman	—spam— Subs Need software? Click here.	9/20/2004 8:43 AM
Shelby Lundy	—spam— Paying too much for your Insurance??	9/20/2004 2:31 PM
Rubin Corbin	—spam— Online ordering is the greatest	9/20/2004 2:11 PM
Sonja Hathaway	—spam— new info	9/20/2004 12:22 PM
Wonderful Daily Savin...	—spam— Multiple ways to get home loans	9/20/2004 10:56 AM
Dick Rucker	—spam— Hiya	9/20/2004 9:30 AM
Rene Clement	—spam— Hi there	9/20/2004 1:17 PM
No cost Laptop	—spam— Find out how to get a Free IBM Thinkpad!	9/20/2004 2:36 PM
Eric Cline	—spam— Carole why can't you call me back?	9/20/2004 12:27 PM
nigel katan	—spam— Relief from pa/in event	9/17/2004 7:23 PM
Bob Allen	—spam— Right out of the TV studio audience	
alexa ramirez	RE: You can become a legally ordained minister	

Deletes the selected messages.



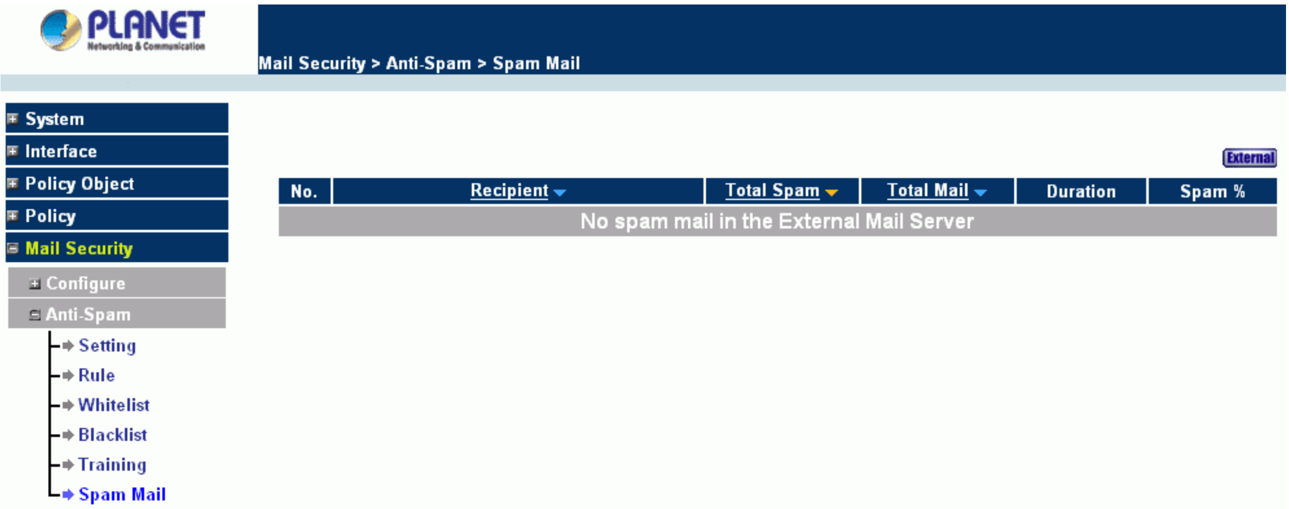
There are no items in this view.

There are no contacts to display. Click on Contacts to create a new contact.

0 message(s), 0 unread

4.5.2.6 Spam Mail

This item will show the top chart that represents the received and sent spam mail from recipient. In **Top Total Spam** report, you can choose to display the scanned mails that sent to **Internal Mail Server** or received from **External Mail Server**. It also can sort the mail according to **Recipient**, **Total Spam** and **Total Mail**.

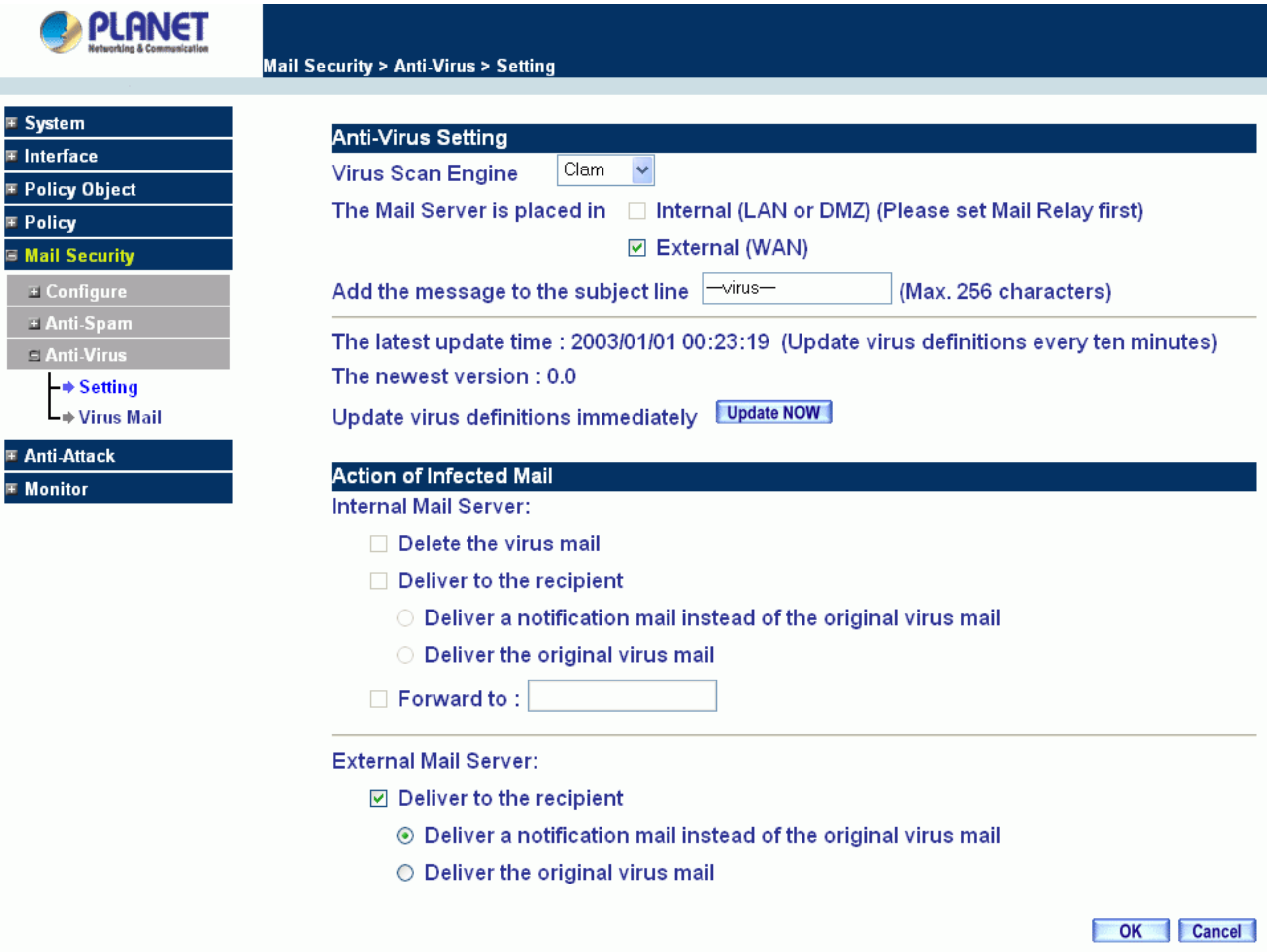


No.	Recipient	Total Spam	Total Mail	Duration	Spam %
No spam mail in the External Mail Server					

4.5.3 Anti-Virus

CS-500 built-in Clam virus scanning engine can protect your LAN network from being infected virus.

4.5.3.1 Setting



Anti-Virus Setting

Virus Scan Engine: Clam

The Mail Server is placed in ☐ Internal (LAN or DMZ) (Please set Mail Relay first) ☑ External (WAN)

Add the message to the subject line: —virus— (Max. 256 characters)

The latest update time : 2003/01/01 00:23:19 (Update virus definitions every ten minutes)

The newest version : 0.0

Update virus definitions immediately

Action of Infected Mail

Internal Mail Server:

☐ Delete the virus mail

☐ Deliver to the recipient

○ Deliver a notification mail instead of the original virus mail

○ Deliver the original virus mail

☐ Forward to :

External Mail Server:

☑ Deliver to the recipient

● Deliver a notification mail instead of the original virus mail

○ Deliver the original virus mail

Definition:

Virus Scan Engine: Select **Clam** to enable Anti-virus function or Select **Disable** to disable it..

The Mail Server is placed in Internal (LAN or DMZ) or External (WAN): Select to choose the location of the mail server.

Add the message to the subject line: If the mail has been filtered to the virus mail, CS-500 will add a message in the mail’s subject. You can configure the message you want, by default, it will be add “VIRUS” in the subject.

Update virus definitions immediately: Press **Update Now** to update CS-500 virus database.

Action of Infected Mail: When CS-500 filters the infected mail, there are three kinds of actions for Internal Mail Server and one action for External Mail server to arrange the infected mail:

Delete the virus mail: If select this option, the virus mail will be deleted without any notification.

Deliver to the recipient: This action is available for Internal Mail Server and External Mail Server setting.

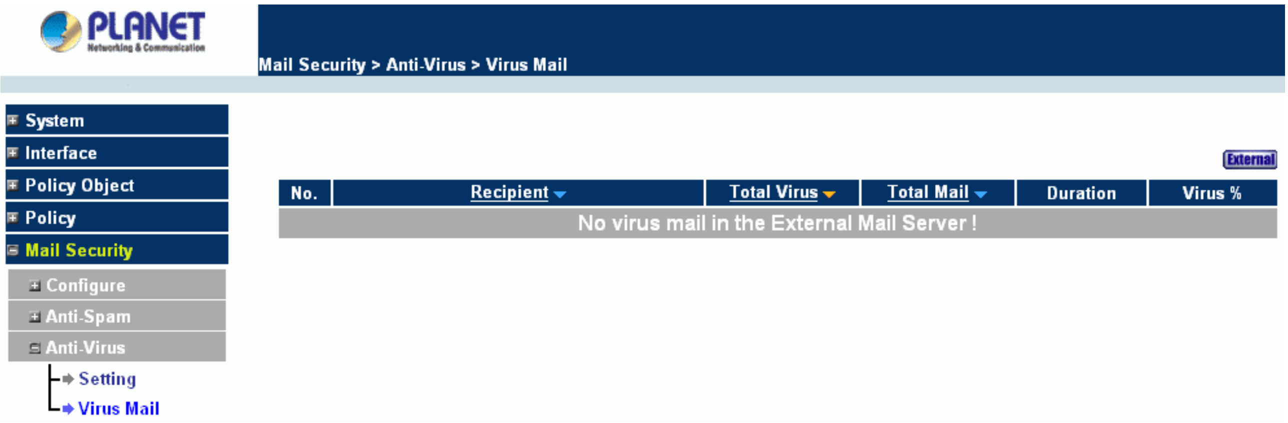
Deliver a notification mail instead of the original virus mail: Recipient will only receive a notification, and virus mail will be deleted.

Deliver the original virus mail: Recipient will receive the original virus mail, the virus will not be arranged, but CS-500 will add a “VIRUS” message at the subject.

Forward to: You can configure CS-500 to forward virus mail to a specific mail account; it will be easily to manage the infected mail.

4.5.3.2 Virus Mail

This item will show the top chart that represents the received and sent virus mail from recipient. In **Top Total Virus** report, you can choose to display the scanned mails that sent to **Internal Mail Server** or received from **External Mail Server**. It also can sort the mail according to Recipient, Total Virus and Total Mail.



No.	Recipient	Total Virus	Total Mail	Duration	Virus %
No virus mail in the External Mail Server !					

4.6 IDP

CS-500 can aim at abnormal traffic and packets content to inspect, alert, and handle by the obstructive, separateness, interference, or alarm to administrator, to prevent suspicious program invades the host. So when CS-500 detects the attack behavior come from internal or external, it can provide the protection to network and obstruct to the attack behavior, let the network can still work normally and increase the information transmission security.

4.6.1 Setting

- It can update signature definitions for every 120 minutes. Or update signature definitions immediately. It will show the update time and version at the same time.
- It can detect virus to the file which have no encryption and compression.

Note: User can test if CS-500 can connect to IDP server to update the signature definitions on internet by **Test** function.

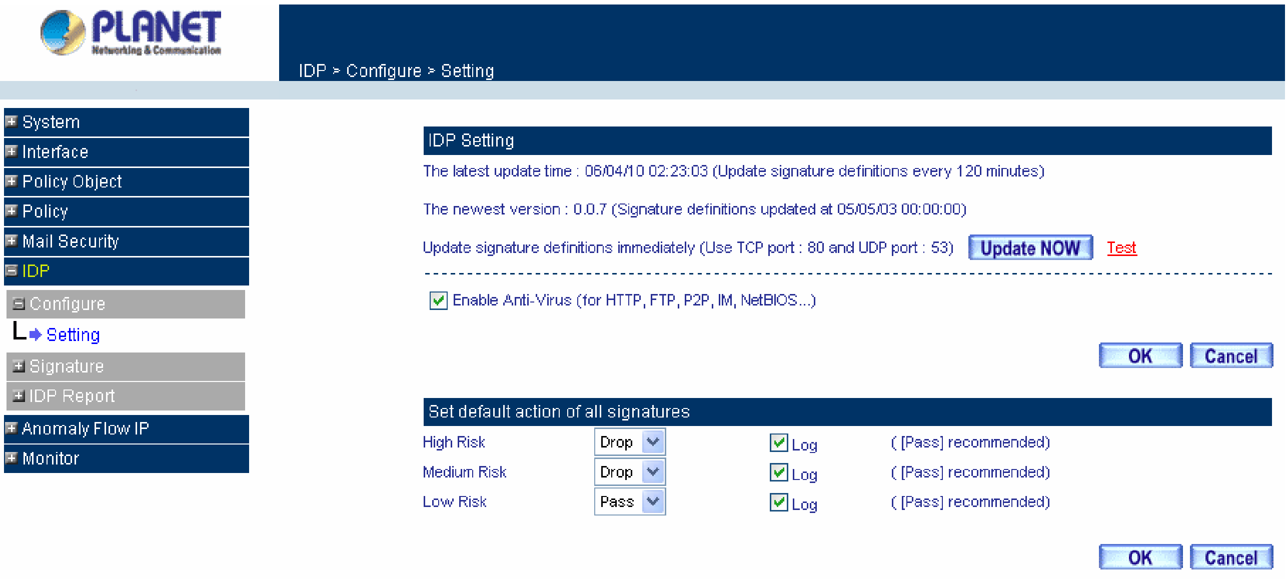
Set default action of all signatures:

- According to attack behavior's threat to divide: **High Risk**, **Medium Risk**, and **Low Risk**. The different risk attack behavior can be handled by the pass, drop, and log action.

  - Add the following settings in this function:

    1. Select **Enable Anti-Virus** (Disable Anti-virus function will abate the IDP function in virus protection).

2. Click **OK**.
3. **High Risk**: Select drop and log function.
4. **Medium Risk**: Select drop and log function.
5. **Low Risk**: Select pass and log function.
6. Click **OK**.
7. Enable **IDP** function in policy.



IDP Setting

The latest update time : 06/04/10 02:23:03 (Update signature definitions every 120 minutes)

The newest version : 0.0.7 (Signature definitions updated at 05/05/03 00:00:00)

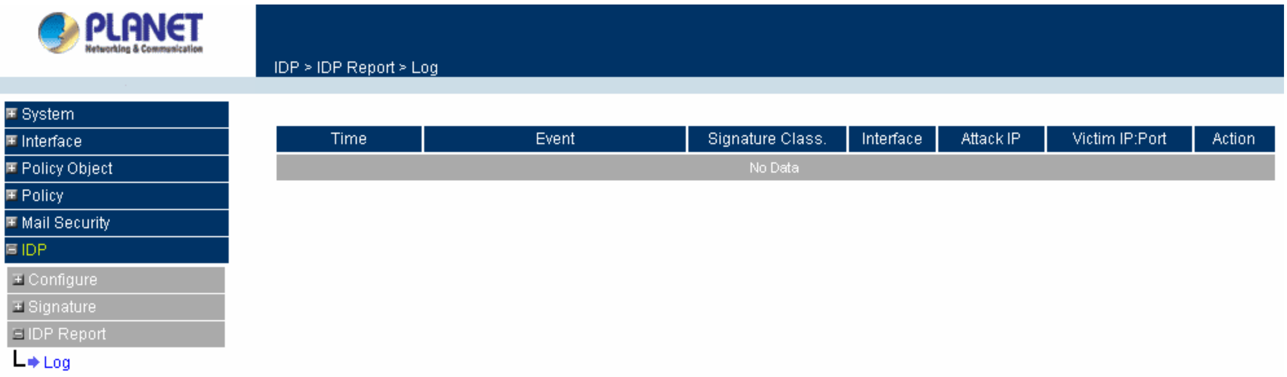
Update signature definitions immediately (Use TCP port : 80 and UDP port : 53)

☑ Enable Anti-Virus (for HTTP, FTP, P2P, IM, NetBIOS...)

Set default action of all signatures

High Risk	Drop	☑ Log	([Pass] recommended)
Medium Risk	Drop	☑ Log	([Pass] recommended)
Low Risk	Pass	☑ Log	([Pass] recommended)

- When the attack behavior matches the signature, CS-500 will produce log as follows in **Log** function of **IDP Report.**



Time	Event	Signature Class.	Interface	Attack IP	Victim IP:Port	Action
No Data						

4.6.2 Signature

Provide relative compare rule to different attack behavior, include three sections: **Anomaly, Pre-defined** and **Custom**.

Anomaly:

Anomaly signature can allow user to define the signature, in order to detect and prevent the irregular attack behavior. Take **Syn Flood** as the example:

Definition:

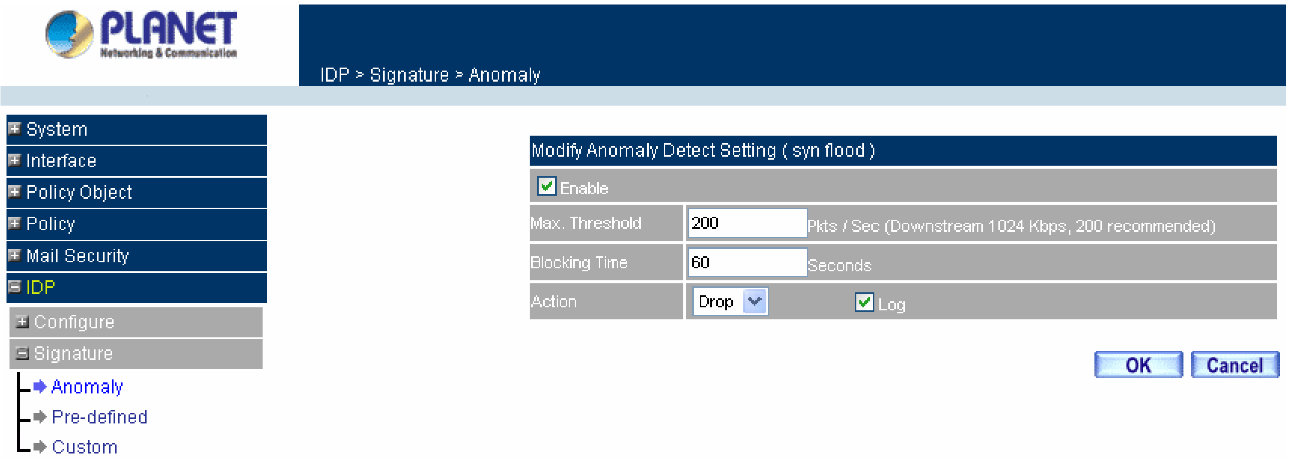
Enable: Check to enable the protection for Syn Flood signature.

Max. Threshold □ Pkts / Sec: Configure the value to define the **Syn Flood** signature.

Blocking Time: Set up the timing to block the attacked connection. The function is available when the **Action** sets to **Drop**.

Action: When the packets match the signature, select **Pass** to pass the packets, or select **Drop** to discard the packets.

Log: Check **Log** function to record the log in **IDP Report**.



IDP > Signature > Anomaly

Modify Anomaly Detect Setting (syn flood)	
☑ Enable	
Max. Threshold	200 Pkts / Sec (Downstream 1024 Kbps, 200 recommended)
Blocking Time	60 Seconds
Action	Drop ☑ Log

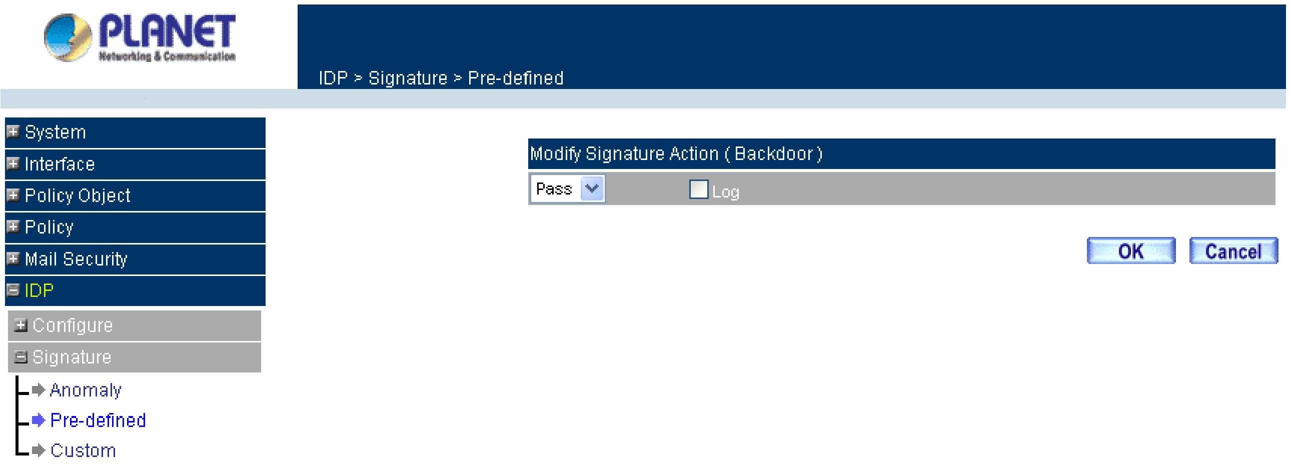
Pre-defined:

Pre-defined signatures can detect and prevent to intrusive pattern which can be discovered at present. These signatures can not be modified and deleted.

Definition:

Action: Select **Pass** to pass the packets, or select **Drop** to discard the packets.

Log: Check **Log** function to record the log in **IDP Report**.



IDP > Signature > Pre-defined

Modify Signature Action (Backdoor)

Pass □ Log

Custom:

Custom signatures can allow user to create the signature according to their requirement, works to detect and prevent the internal and external attack behavior which are not including in **Pre-defined** signatures.

Definition:

Name: The System Manager can name the signature.

Protocol: Select the protocol which wants to be detected and prevented, it can be divided: TCP, UDP, ICMP and IP.

Source Port: Configure the port number that is used to attack the PC. (The range can be from 0 to 65535).

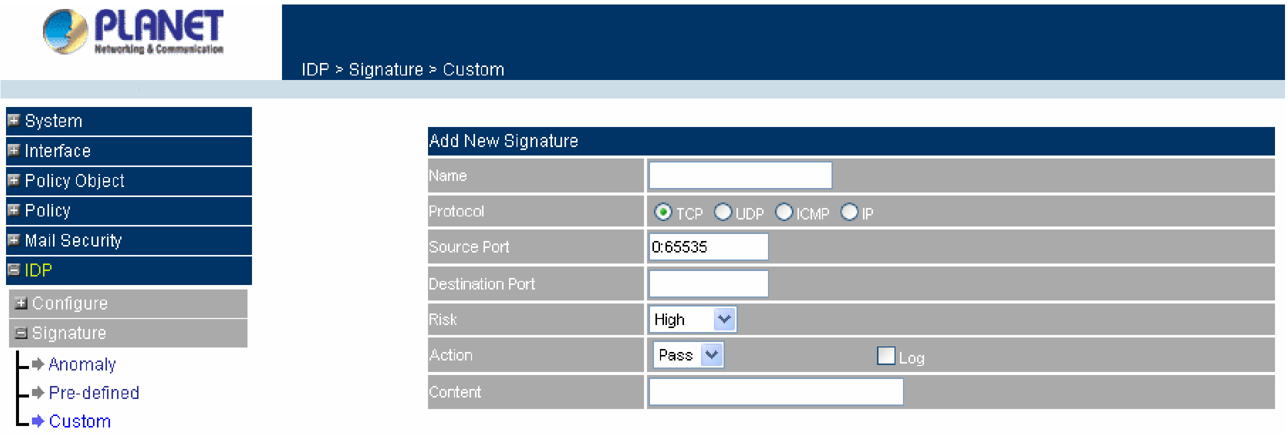
Destination Port: Configure the port number that the client PC is used to be attacked.

Risk: Define the threat about attack packets.

Action: Select **Pass** to pass the packets, or select **Drop** to discard the packets.

Log: Check **Log** function to record the log in **IDP Report**.

Content: Define the attack packets content.



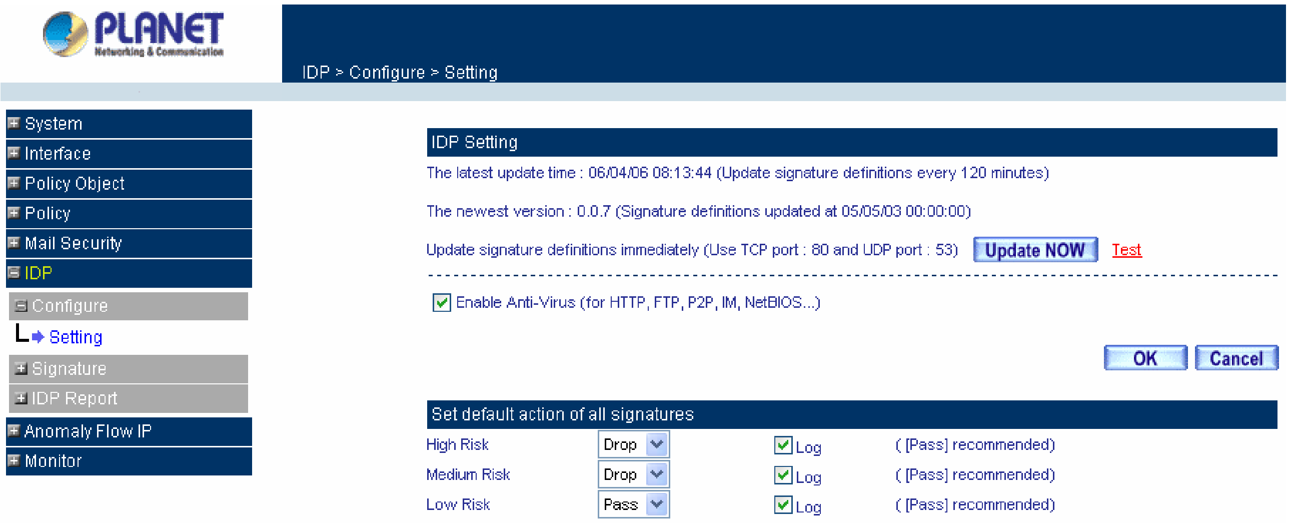
IDP > Signature > Custom

Add New Signature

Name	
Protocol	● TCP ○ UDP ○ ICMP ○ IP
Source Port	0:65535
Destination Port	
Risk	High
Action	Pass □ Log
Content	

EX. Use Pre-defined and Custom signature settings to detect and prevent attack behaviors

STEP 1. Enter the following setting in **Setting** of **Configure** function.



IDP > Configure > Setting

IDP Setting

The latest update time : 06/04/06 08:13:44 (Update signature definitions every 120 minutes)

The newest version : 0.0.7 (Signature definitions updated at 05/05/03 00:00:00)

Update signature definitions immediately (Use TCP port : 80 and UDP port : 53)

☑ Enable Anti-Virus (for HTTP, FTP, P2P, IM, NetBIOS...)

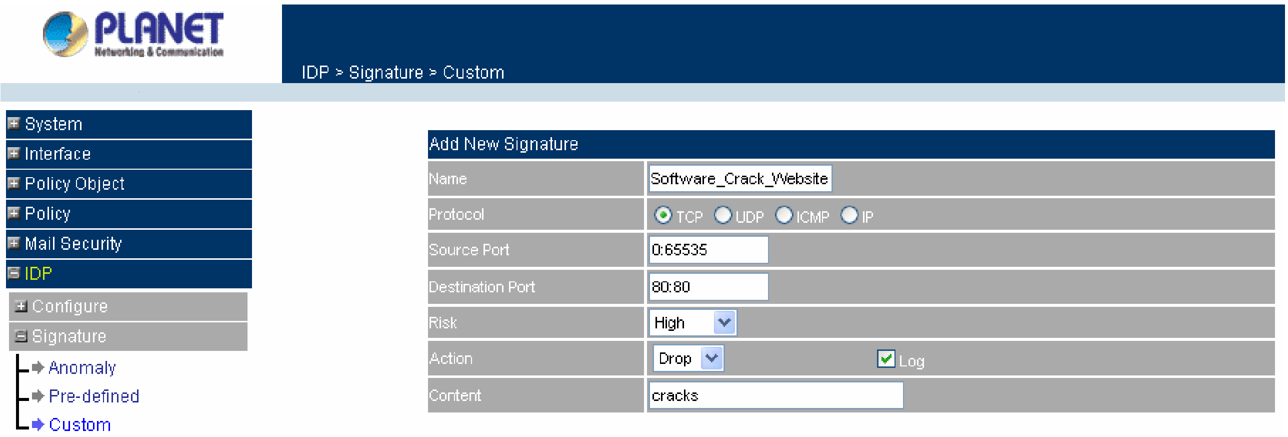
Set default action of all signatures

High Risk	Drop	☑ Log	([Pass] recommended)
Medium Risk	Drop	☑ Log	([Pass] recommended)
Low Risk	Pass	☑ Log	([Pass] recommended)

STEP 2. Enter the following setting in **Custom** of **Signature** function:

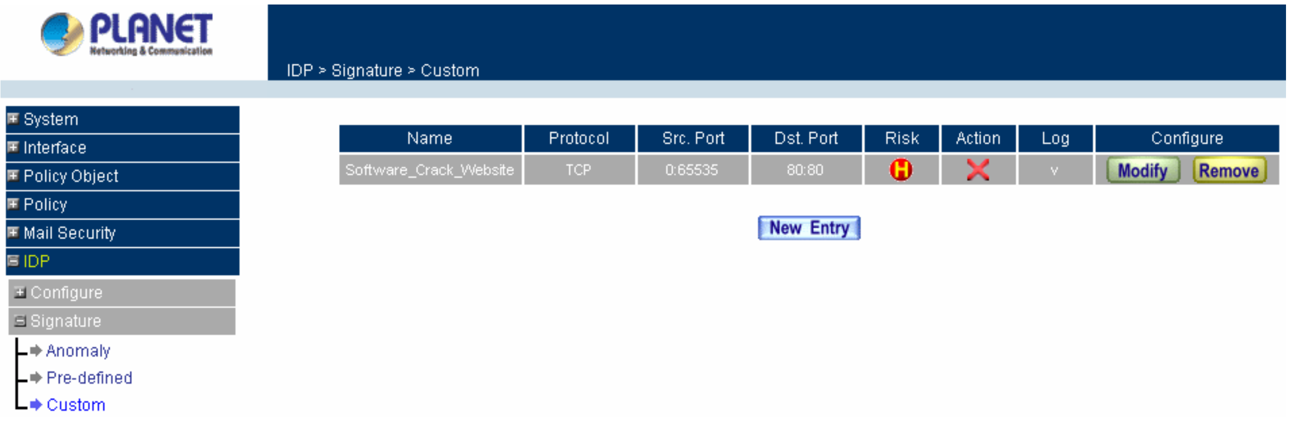
- Click **New Entry**.
- **Name**: Enter Software_Crack_Website.
- **Protocol**: Select TCP.
- **Source Port**: Enter 0:65535.

- **Destination Port**: Enter 80:80.
- **Risk**: Select High.
- **Action**: Select Drop and enable Log function.
- **Content**: Enter cracks.



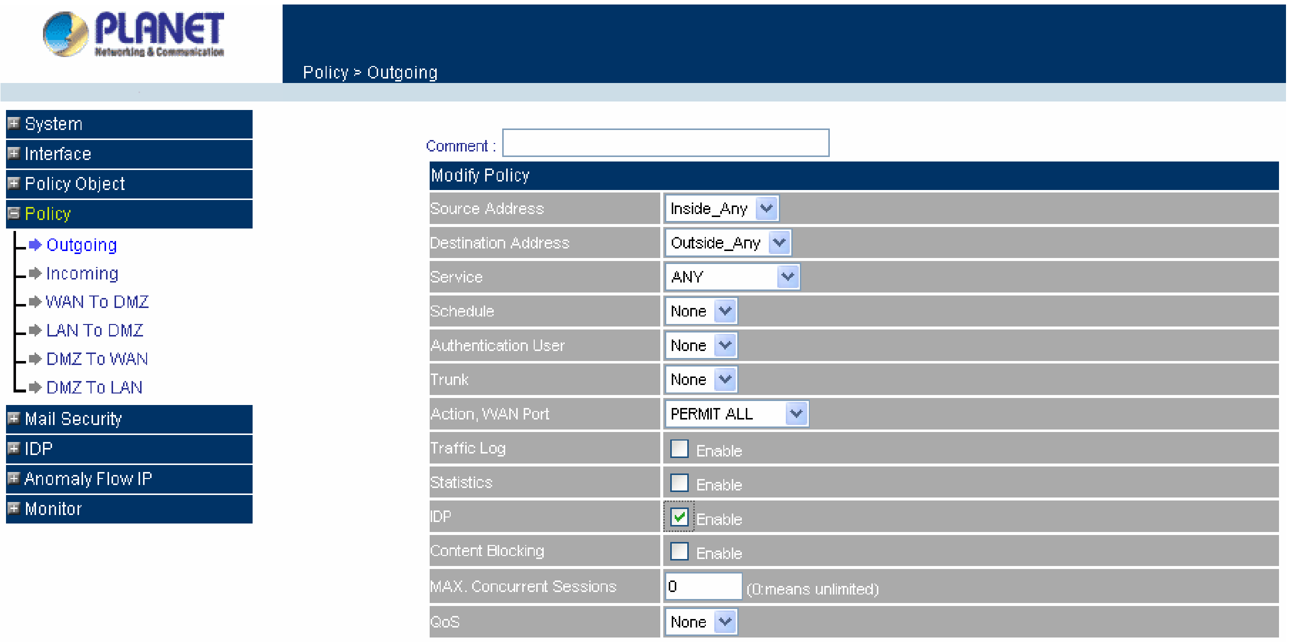
Add New Signature	
Name	Software_Crack_Website
Protocol	● TCP ○ UDP ○ ICMP ○ IP
Source Port	0:65535
Destination Port	80:80
Risk	High
Action	Drop ☑ Log
Content	cracks

Click OK to finish the IDP setting.



Name	Protocol	Src. Port	Dst. Port	Risk	Action	Log	Configure
Software_Crack_Website	TCP	0:65535	80:80	H	✗	v	Modify Remove

STEP 3. Enter the following settings in **Outgoing Policy** to enable the **IDP** function:



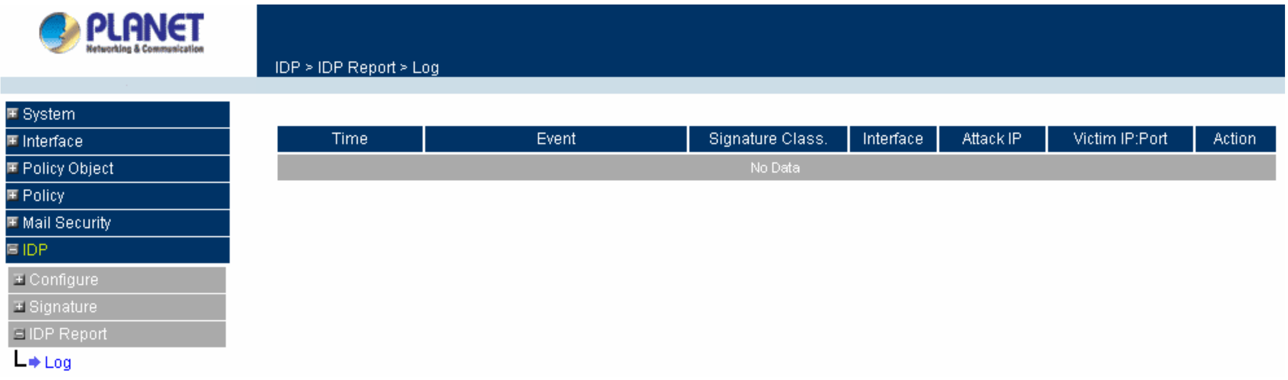
Comment :

Modify Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
Trunk	None
Action, WAN Port	PERMIT ALL
Traffic Log	□ Enable
Statistics	□ Enable
IDP	☑ Enable
Content Blocking	□ Enable
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None

4.6.3 IDP Report

CS-500 can make intrusion detection and prevention record to a Log report, and allow administrator to know the network security status for the overall network.

STEP 1. In **Log** of **IDP Report** function, it will display the situation about intrusion detection and prevention of CS-500.



Time	Event	Signature Class.	Interface	Attack IP	Victim IP:Port	Action
No Data						

Icon Definition:

1. **Action:**

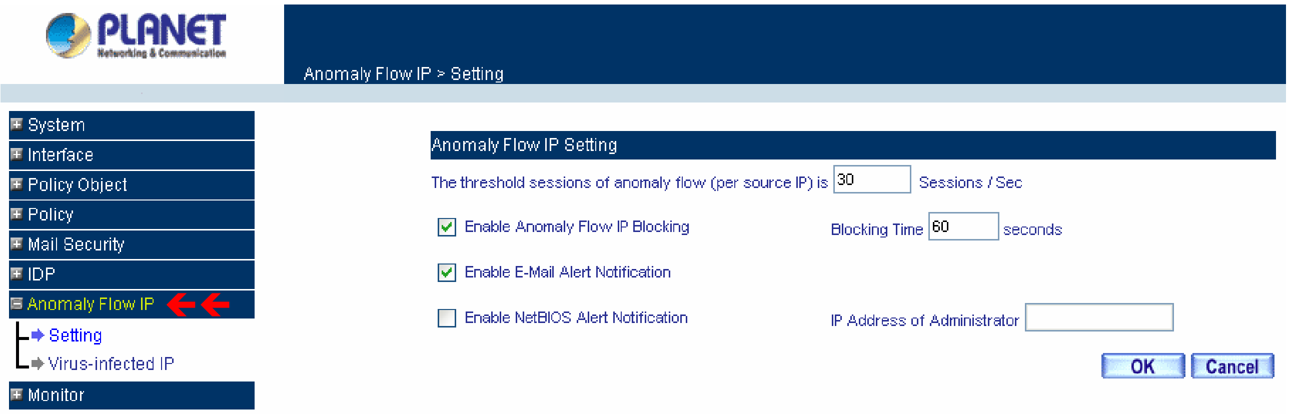
➡	✗
Pass	Drpo

2. **Risk:**

H	M	L
High Risk	Medium Risk	Low Risk

4.7 Anomaly Flow IP

The Administrator can enable the device's auto detect functions for Anomaly Flow IP attacking the local network. When abnormal conditions occur, CS-500 will send an e-mail alert to notify the Administrator, and also display warning messages in the Virus-infected IP window.



Anomaly Flow IP Setting

The threshold sessions of anomaly flow (per source IP) is 30 Sessions / Sec

☑ Enable Anomaly Flow IP Blocking   Blocking Time 60 seconds

☑ Enable E-Mail Alert Notification

□ Enable NetBIOS Alert Notification   IP Address of Administrator

Anomaly Flow IP Settings

- **Enable Anomaly Flow IP Blocking**: Select this option to enable the Anomaly Flow IP blocking function. Once the Anomaly Flow IP attacked is detected, it will block the connection for user-drefined blocking time.
- **Enable E-mail Alert Notification:** When Anomaly Flow IP attacked is detected, send alert e-mail to administrator by using e-mail address defined on System -> Setting.
- **Enable NetBIOS Alert Notification:** When Anomaly Flow IP attacked is detected, send alart message to administrator by using "Net send" command.

After enabling the needed options, click OK to activate the changes.

4.8 Monitor

CS-500 provides varied of information that can be used to check the status.

4.8.1 Log

The Content Security Gateway supports traffic logging and event logging to monitor and record services, connection times, and the source and destination network address. The Administrator may also download the log files for backup purposes. The Administrator mainly uses the Log menu to monitor the traffic passing through the Content Security Gateway.

What is Log?

Log records all connections that pass through the Content Security Gateway's control policies. Traffic log's parameters are setup when setting up control policies. Traffic logs record the details of packets such as the start and stop time of connection, the duration of connection, the source address, the destination address and services requested, for each control policy. Event logs record the contents of System Configuration changes made by the Administrator such as the time of change, settings that change, the IP address used to log on, etc.

How to use the Log

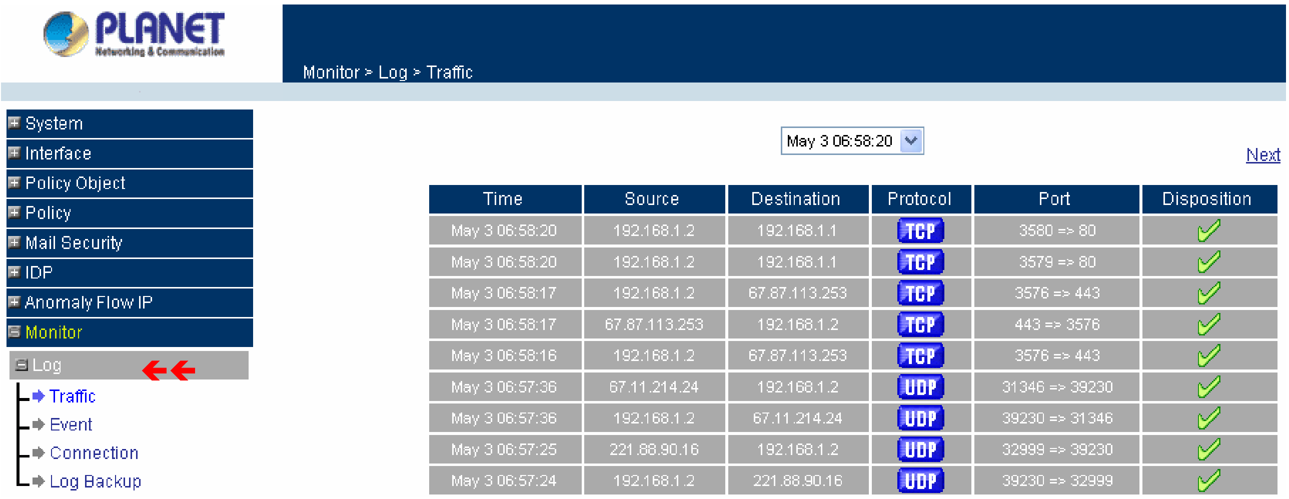
The Administrator can use the log data to monitor and manage the device and the networks. The Administrator can view the logged data to evaluate and troubleshoot the network, such as pinpointing the source of traffic congestions.

4.8.1.1 Traffic

The Administrator queries the Content Security Gateway for information, such as source address, destination address, start time, and Protocol port of all connections.

Entering the Traffic Log window

Step 1. Click the **Traffic** option under **Log** menu to enter the Traffic Log window.



Time	Source	Destination	Protocol	Port	Disposition
May 3 06:58:20	192.168.1.2	192.168.1.1	TCP	3580 => 80	✓
May 3 06:58:20	192.168.1.2	192.168.1.1	TCP	3579 => 80	✓
May 3 06:58:17	192.168.1.2	67.87.113.253	TCP	3576 => 443	✓
May 3 06:58:17	67.87.113.253	192.168.1.2	TCP	443 => 3576	✓
May 3 06:58:16	192.168.1.2	67.87.113.253	TCP	3576 => 443	✓
May 3 06:57:36	67.11.214.24	192.168.1.2	UDP	31346 => 39230	✓
May 3 06:57:36	192.168.1.2	67.11.214.24	UDP	39230 => 31346	✓
May 3 06:57:25	221.88.90.16	192.168.1.2	UDP	32999 => 39230	✓
May 3 06:57:24	192.168.1.2	221.88.90.16	UDP	39230 => 32999	✓

Traffic Log Table

The table in the Traffic Log window displays current System statuses:

Definition:

- **Time**: The start time of the connection.
- **Source:** IP address of the source network of the specific connection.
- **Destination:** IP address of the destination network of the specific connection.
- **Protocol:** Protocol type of the specific connection.
- **Port:** Port number of the specific connection.
- **Disposition:** Accept or Deny.

Downloading the Traffic Logs

The Administrator can backup the traffic logs regularly by downloading it to the computer.

Step 1. In the Traffic Log window, click the **Download Logs** button at the bottom of the screen.

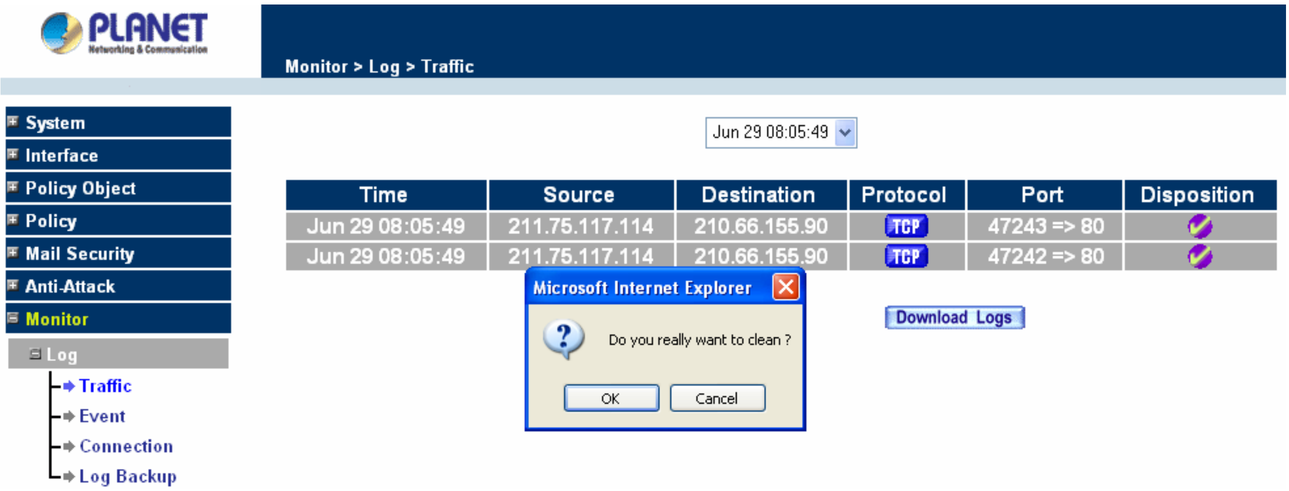
Step 2. Follow the File Download pop-up window to save the traffic logs into a specified directory on the hard drive.

Clearing the Traffic Logs

The Administrator may clear on-line logs to keep just the most updated logs on the screen.

Step 1. In the Traffic Log window, click the **Clear Logs** button at the bottom of the screen.

Step 2. In the Clear Logs pop-up box, click **Ok** to clear the logs or click **Cancel** to cancel it.



Time	Source	Destination	Protocol	Port	Disposition
Jun 29 08:05:49	211.75.117.114	210.66.155.90	TCP	47243 => 80	✓
Jun 29 08:05:49	211.75.117.114	210.66.155.90	TCP	47242 => 80	✓

Microsoft Internet Explorer

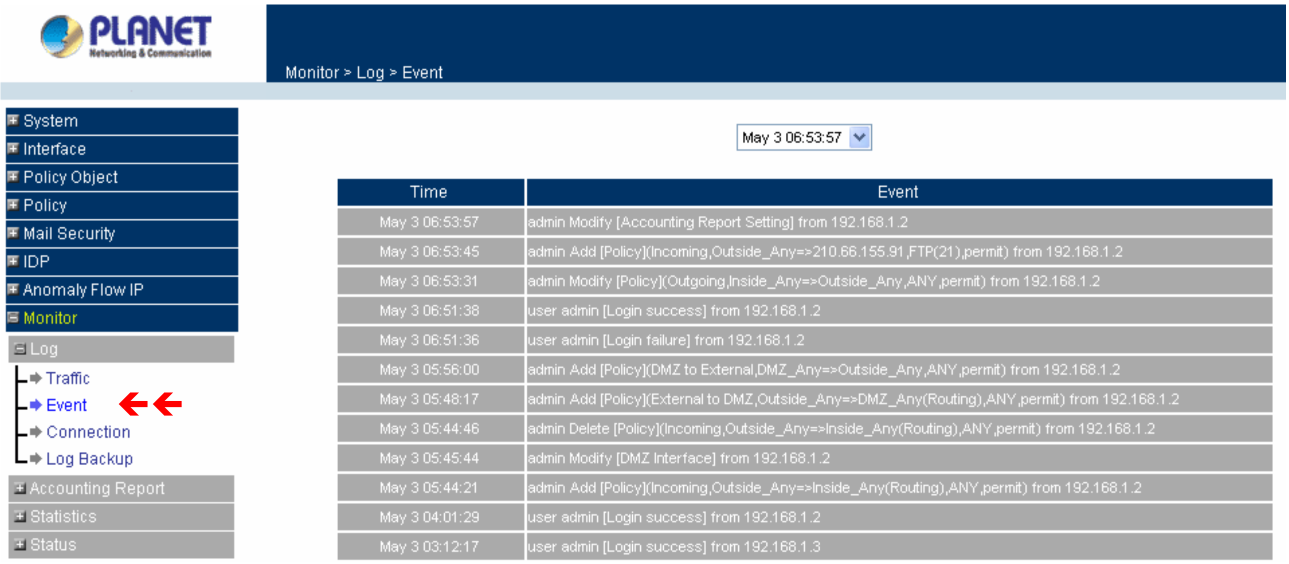
Do you really want to clean ?

4.8.1.2 Event

When the Content Security Gateway WAN detects events, the Administrator can get the details, such as time and description of the events from the Event Logs.

Entering the Event Log window

Step 1. Click the **Event Log** option under the **Log** menu and the Event Log window will appear.



Time	Event
May 3 06:53:57	admin Modify [Accounting Report Setting] from 192.168.1.2
May 3 06:53:45	admin Add [Policy](Incoming,Outside_Any=>210.66.155.91,FTP(21),permit) from 192.168.1.2
May 3 06:53:31	admin Modify [Policy](Outgoing,Inside_Any=>Outside_Any,ANY,permit) from 192.168.1.2
May 3 06:51:38	user admin [Login success] from 192.168.1.2
May 3 06:51:36	user admin [Login failure] from 192.168.1.2
May 3 05:56:00	admin Add [Policy](DMZ to External,DMZ_Any=>Outside_Any,ANY,permit) from 192.168.1.2
May 3 05:48:17	admin Add [Policy](External to DMZ,Outside_Any=>DMZ_Any(Routing),ANY,permit) from 192.168.1.2
May 3 05:44:46	admin Delete [Policy](Incoming,Outside_Any=>Inside_Any(Routing),ANY,permit) from 192.168.1.2
May 3 05:45:44	admin Modify [DMZ Interface] from 192.168.1.2
May 3 05:44:21	admin Add [Policy](Incoming,Outside_Any=>Inside_Any(Routing),ANY,permit) from 192.168.1.2
May 3 04:01:29	user admin [Login success] from 192.168.1.2
May 3 03:12:17	user admin [Login success] from 192.168.1.3

Step 2. The table in the Event Log window displays the time and description of the events.

- **Time:** time when the event occurred.
- **Event:** description of the event.

Downloading the Event Logs

Step 1. In the Event Log window, click the Download Logs button at the bottom of the screen.

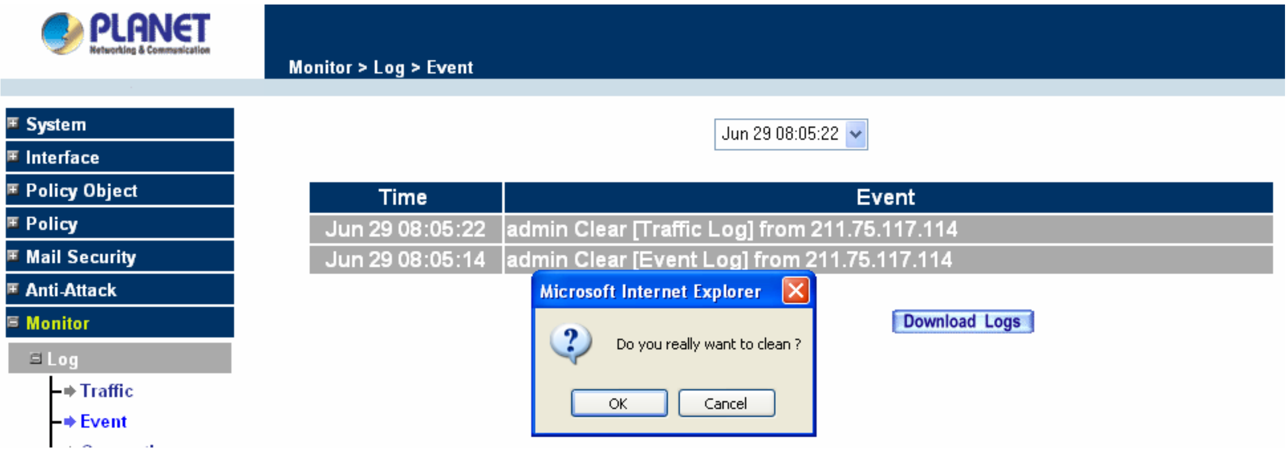
Step 2. Follow the File Download pop-up window to save the event logs into a specific directory on the hard drive.

Clearing the Event Logs

The Administrator may clear on-line event logs to keep just the most updated logs on the screen.

Step 1. In the Event Log window, click the Clear Logs button at the bottom of the screen.

Step 2. In the Clear Logs pop-up box, click **OK** to clear the logs or click **Cancel** to cancel it.

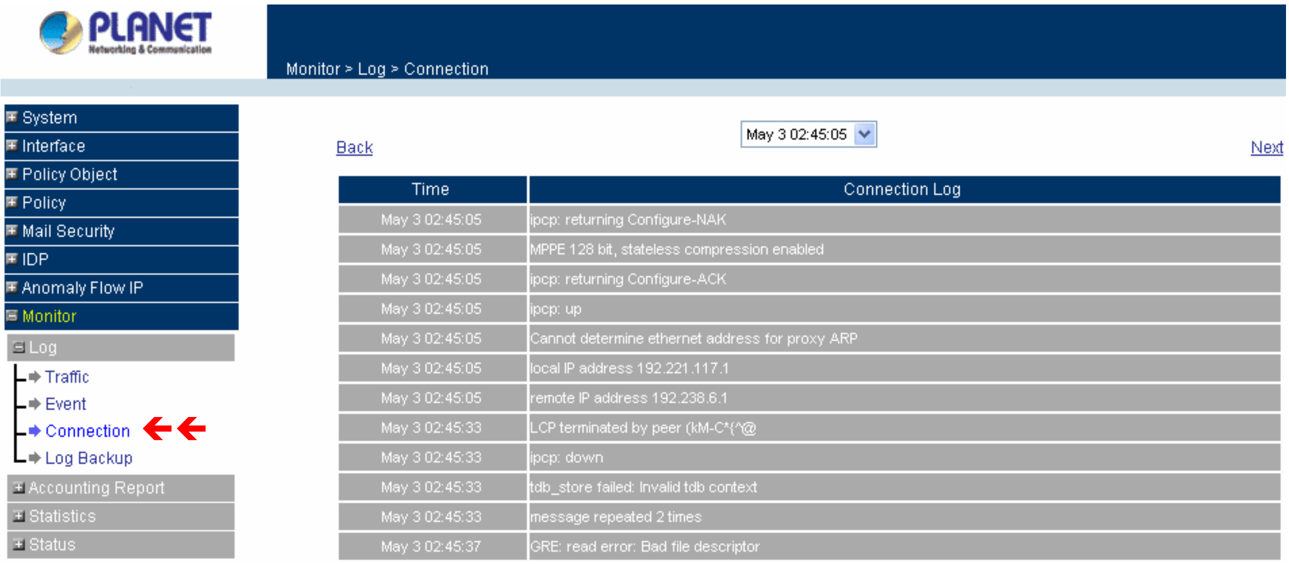


Do you really want to clean ?

Time	Event
Jun 29 08:05:22	admin Clear [Traffic Log] from 211.75.117.114
Jun 29 08:05:14	admin Clear [Event Log] from 211.75.117.114

4.8.1.3 Connection

Click Log in the menu bar on the left hand side, and then select the sub-selection Connection Log.



Time	Connection Log
May 3 02:45:05	ipcp: returning Configure-NAK
May 3 02:45:05	MPPE 128 bit, stateless compression enabled
May 3 02:45:05	ipcp: returning Configure-ACK
May 3 02:45:05	ipcp: up
May 3 02:45:05	Cannot determine ethernet address for proxy ARP
May 3 02:45:05	local IP address 192.221.117.1
May 3 02:45:05	remote IP address 192.238.6.1
May 3 02:45:33	LCP terminated by peer (kM-C*{^@
May 3 02:45:33	ipcp: down
May 3 02:45:33	tdb_store failed: Invalid tdb context
May 3 02:45:33	message repeated 2 times
May 3 02:45:37	GRE: read error: Bad file descriptor

Definition:

Time: The start and end time of connection.

Connection Log: Event description during connection.

Download Logs

Step 1. Click **Log** in the menu bar on the left hand side and then select the sub-selection **Connection Log**.

Step 2. In Connection Log window, click the **Download Logs** button.

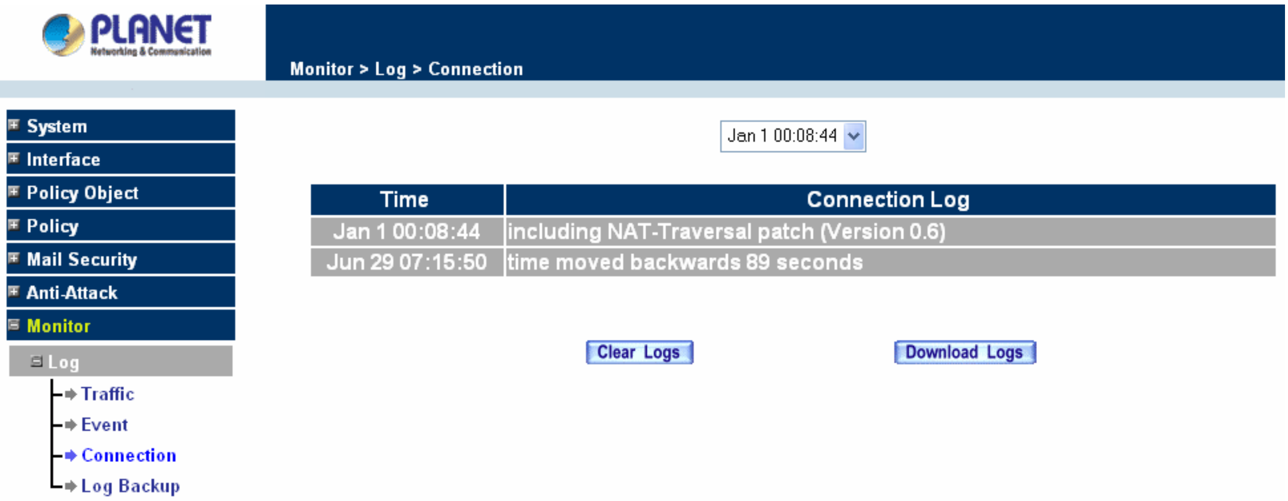
Step 3. In the Download Logs window, save the logs to the specified location.

Clear Logs

Step 1. Click **Log** in the menu bar on the left hand side, and then select the sub-selection **Connection Logs**.

Step 2. In Connection Log window, click the **Clear Logs** button.

Step 3. In Clear Logs window, click **OK** to clear the logs or click **Cancel** to discard changes.



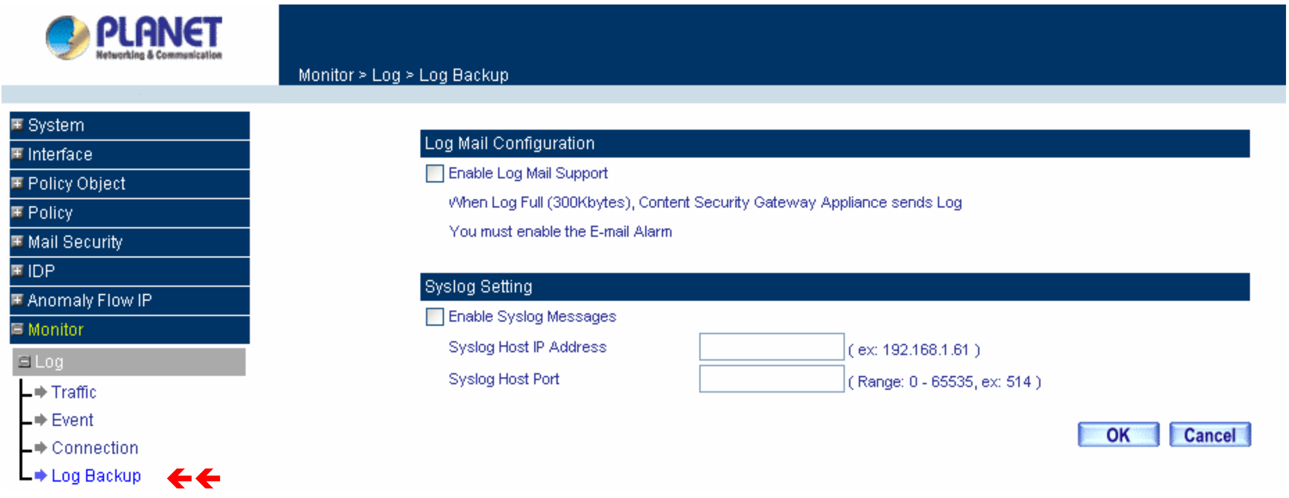
Monitor > Log > Connection

Jan 1 00:08:44

Time	Connection Log
Jan 1 00:08:44	including NAT-Traversal patch (Version 0.6)
Jun 29 07:15:50	time moved backwards 89 seconds

4.8.1.4 Log Backup

Click **Log →Log Backup**.



Monitor > Log > Log Backup

Log Mail Configuration

□ Enable Log Mail Support

When Log Full (300Kbytes), Content Security Gateway Appliance sends Log

You must enable the E-mail Alarm

Syslog Setting

□ Enable Syslog Messages

Syslog Host IP Address (ex: 192.168.1.61)

Syslog Host Port (Range: 0 - 65535, ex: 514)

Log Mail Configuration: When the Log Mail files accumulated up to 300Kbytes, router will notify administrator by email with the traffic log and event log.

NOTE: Before enabling this function, you have to configure E-mail Settings in System -> Settings.

Syslog Settings: If you enable this function, system will transmit the Traffic Log and the Event Log simultaneously to the server which supports Syslog function.

NOTE: To restart Connection Log, click the **Refresh** button on the right hand side in Log window.

Enable Log Mail Support & Syslog Message

Log Mail Configuration /Enable Log Mail Support

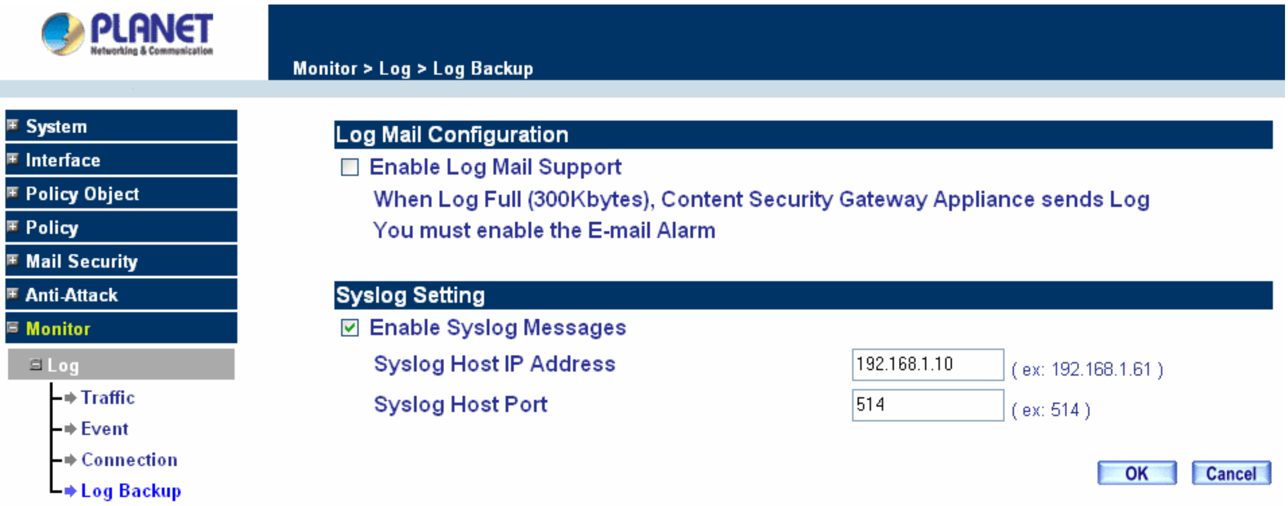
Step 1. Firstly, go to **Admin** –Select **Enable E-mail Alert Notification** under **E-Mail Settings**. Enter the e-mail address to receive the alarm notification. Click **OK**.

Step 2. Go to **LOG →Log Backup.** Check to enable **Log Mail Support.** Click **OK.**

System Settings/Enable Syslog Message

Step 1. Check to enable Syslog Message. Enter the Host IP Address and Host Port number to receive the Syslog message.

Step 2. Click **OK**.



Log Mail Configuration

□ Enable Log Mail Support

When Log Full (300Kbytes), Content Security Gateway Appliance sends Log

You must enable the E-mail Alarm

Syslog Setting

☑ Enable Syslog Messages

Syslog Host IP Address 192.168.1.10 (ex: 192.168.1.61)

Syslog Host Port 514 (ex: 514)

Disable Log Mail Support & Syslog Message

Step 1. Go to **LOG →Log Backup**. Uncheck to disable Log Mail Support. Click **OK**.

Step 2. Go to **LOG →Log Backup**. Uncheck to disable Settings Message. Click **OK**.

4.8.2 Accounting Report

Accounting Report can be divided into three parts, **Setting**, **Outbound** and **Inbound**.

4.8.2.1 Setting

Select **Setting** to configure what type of Accounting Report will be logged at CS-500. There are three types of report can be select: **Source IP**, **Destination IP** and **Service**.

Outbound Accounting Report: the statistics of the downstream and upstream for the LAN, WAN and all kinds of communication services.

Source IP: Select to record the statistic based on Source IP address.

Destination IP: Select to record the statistic based on Destination IP address.

Service: Select to record the statistic based on Service.

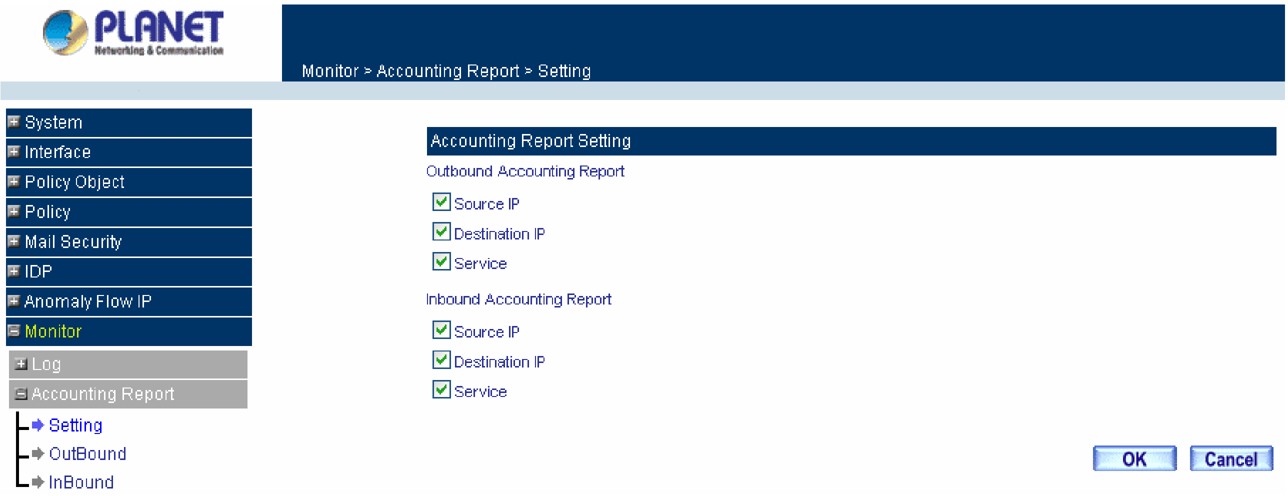
Inbound Accounting Report: the statistics of downstream and upstream for all kinds of communication services; the Inbound Accounting report will be shown when WAN host connects to LAN host via CS-500.

Source IP: Select to record the statistic based on Source IP address.

Destination IP: Select to record the statistic based on Destination IP address.

Service: Select to record the statistic based on Service.

Administrator can use this Accounting Report to inquire the LAN IP users and WAN IP users, and to gather the statistics of Downstream/Upstream, First packet/Last packet/Duration and the service for all of the user's IP that passes through CS-500.



Accounting Report Setting

Outbound Accounting Report

☑ Source IP

☑ Destination IP

☑ Service

Inbound Accounting Report

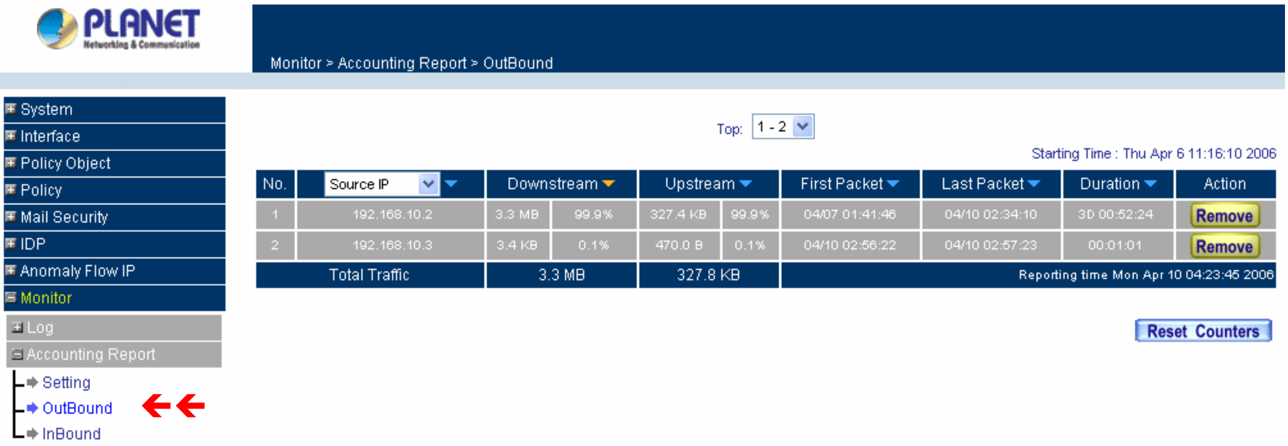
☑ Source IP

☑ Destination IP

☑ Service

4.8.2.2 Outbound

Click the **Accounting Report** function, and then select **Outbound**. There are three options for outbound acounting report: Source IP, Destination IP and Services.



Monitor > Accounting Report > OutBound

Top: 1 - 2

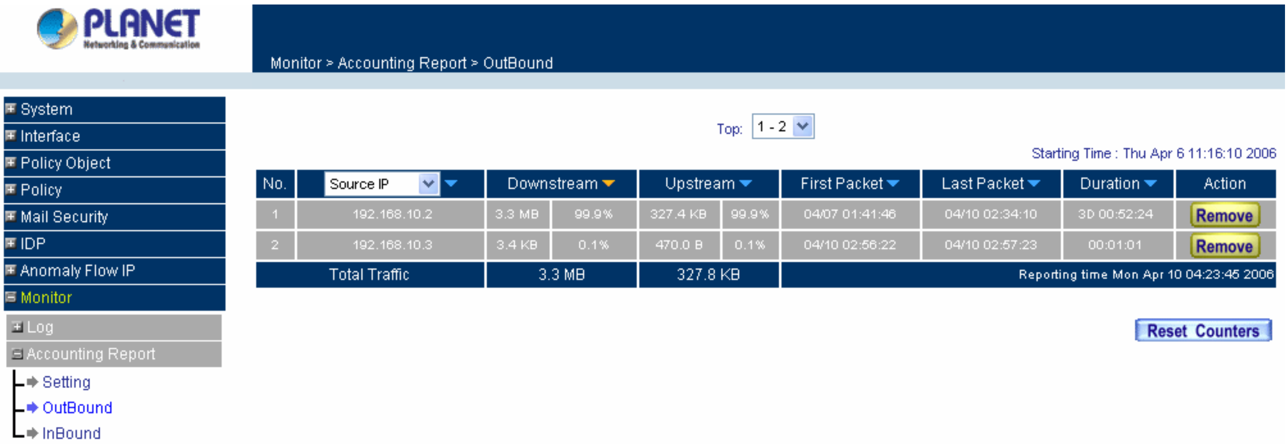
Starting Time : Thu Apr 6 11:16:10 2006

No.	Source IP	Downstream		Upstream		First Packet	Last Packet	Duration	Action
1	192.168.10.2	3.3 MB	99.9%	327.4 KB	99.9%	04/07 01:41:46	04/10 02:34:10	3D 00:52:24	Remove
2	192.168.10.3	3.4 KB	0.1%	470.0 B	0.1%	04/10 02:56:22	04/10 02:57:23	00:01:01	Remove
Total Traffic		3.3 MB		327.8 KB		Reporting time Mon Apr 10 04:23:45 2006			

Reset Counters

Outbound Source IP Accounting Report

Pull down the menu and select **Source IP** to show the outbound source IP accounting report.



Monitor > Accounting Report > OutBound

Top: 1 - 2

Starting Time : Thu Apr 6 11:16:10 2006

No.	Source IP	Downstream		Upstream		First Packet	Last Packet	Duration	Action
1	192.168.10.2	3.3 MB	99.9%	327.4 KB	99.9%	04/07 01:41:46	04/10 02:34:10	3D 00:52:24	Remove
2	192.168.10.3	3.4 KB	0.1%	470.0 B	0.1%	04/10 02:56:22	04/10 02:57:23	00:01:01	Remove
Total Traffic		3.3 MB		327.8 KB		Reporting time Mon Apr 10 04:23:45 2006			

Reset Counters

When LAN users connect to WAN service server through CS-500, all of the Downstream / Upstream / First Packet / Last Packet / Duration log of the source IP will be recorded.

Definition:

Top: Select the data type you want to check. It presents 10 results in one page.

Source IP: The LAN user's IP address connects to CS-500 to access WAN service server.

Downstream: The percentage of downstream and the statistic value of the connection from WAN server to LAN user.

Upstream: The percentage of upstream and the statistic value of the connection from LAN user to WAN server.

First Packet: The time record of the first packet that was sent to WAN service server from LAN user.

Last Packet: The time record of the last packet sent from WAN server and received by the LAN user

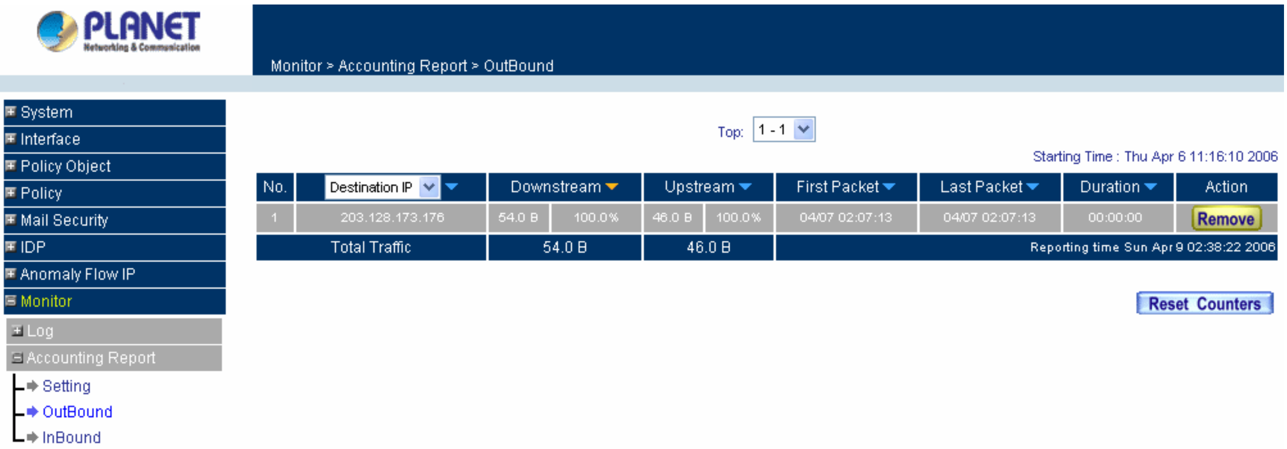
Duration: The time statistic record that started from the first packet and end to the last packet.

Total Traffic: CS-500 will record the sum of upstream/downstream packets from LAN user to WAN service server.

Reset Counters: Click **Reset Counters** button to refresh Accounting Report.

Outbound Destination IP Accounting Report

Pull down the menu and select **Destination IP** to show the outbound destination IP accounting report.



Top: 1 - 1

Starting Time : Thu Apr 6 11:16:10 2006

No.	Destination IP	Downstream		Upstream		First Packet	Last Packet	Duration	Action
1	203.128.173.176	54.0 B	100.0%	46.0 B	100.0%	04/07 02:07:13	04/07 02:07:13	00:00:00	Remove
Total Traffic		54.0 B		46.0 B		Reporting time Sun Apr 9 02:38:22 2006			

Reset Counters

When LAN user connect to WAN service server through CS-500, all of the Downstream / Upstream / First Packet / Last Packet / Duration log of the Destination IP will be recorded.

Definition:

Top: Select the data type you want to check. It presents 10 results in one page.

Destination IP: The WAN Server's IP address.

Downstream: The percentage of downstream and the statistic value of the connection from LAN user to WAN server.

Upstream: The percentage of upstream and the statistic value of the connection from WAN server to LAN user.

First Packet: The time record of the first packet that was sent to LAN user from WAN service server.

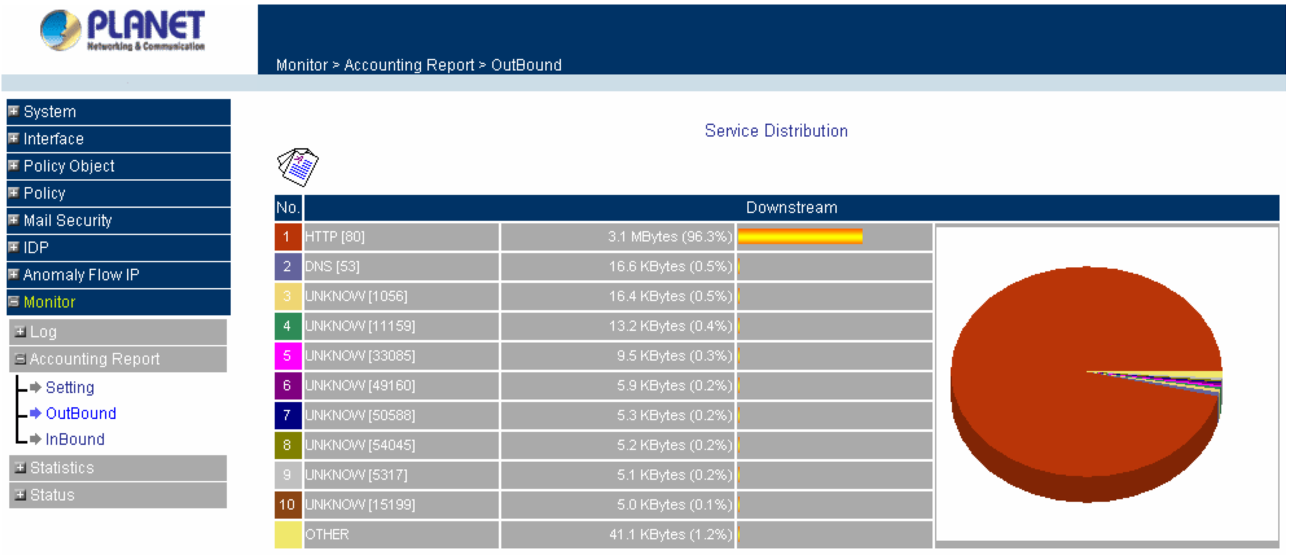
Last Packet: The time record of the last packet sent from LAN user and received by the WAN server

Duration: The time statistic record that started from the first packet and end to the last packet.

Total Traffic: CS-500 will record the sum of upstream/downstream packets from LAN user to WAN service server.

Outbound Service Accounting Report

Pull down the menu and select **Service** to show the outbound service accounting report.



Service Distribution

No.	Downstream		
1	HTTP [80]	3.1 MBytes (96.3%)	
2	DNS [53]	16.6 KBytes (0.5%)	
3	UNKNOW [1056]	16.4 KBytes (0.5%)	
4	UNKNOW [11159]	13.2 KBytes (0.4%)	
5	UNKNOW [33085]	9.5 KBytes (0.3%)	
6	UNKNOW [49160]	5.9 KBytes (0.2%)	
7	UNKNOW [50588]	5.3 KBytes (0.2%)	
8	UNKNOW [54045]	5.2 KBytes (0.2%)	
9	UNKNOW [5317]	5.1 KBytes (0.2%)	
10	UNKNOW [15199]	5.0 KBytes (0.1%)	
	OTHER	41.1 KBytes (1.2%)	

When LAN users connect to WAN Service Server through CS-500, all of the Downstream / Upstream / First Packet / Last Packet / Duration log of the Communication Service will be recorded.

Definitions:

Top: Select the data type you want to check. It presents 10 results in one page.

Service: The report of Communication Service when LAN users connect to WAN service server through CS-500. **(Port)** indicates the protocol port number.

Downstream: The percentage of downstream and the statistic value of the connection from WAN server to LAN user.

Upstream: The percentage of upstream and the statistic value of the connection from LAN user to WAN server.

First Packet: The time record of the first packet that was sent to WAN service server from LAN user.

Last Packet: The time record of the last packet sent from WAN server and received by the LAN user

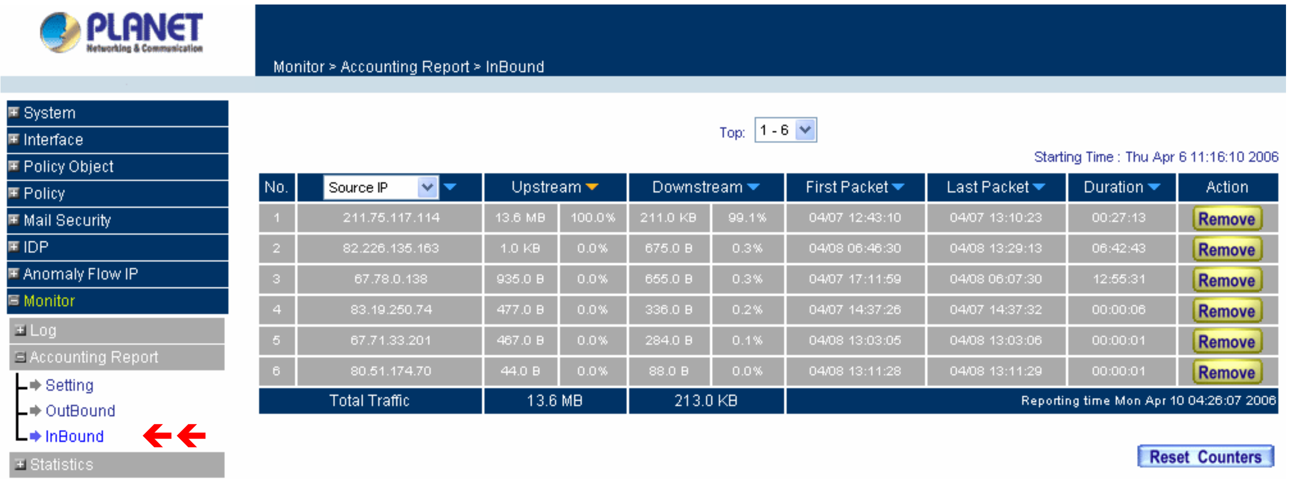
Duration: The time statistic record that started from the first packet and end to the last packet

Total Traffic: CS-500 will record the sum of upstream/downstream packets from LAN user to WAN service server.

NOTE: To correctly display the pizza chart, please install the latest java VM for http://www.java.com.

4.8.2.3 Inbound

Click the **Accounting Report** function, and then select **Inbound**. There are three options for Inbound acounting report: Source IP, Destination IP and Service.



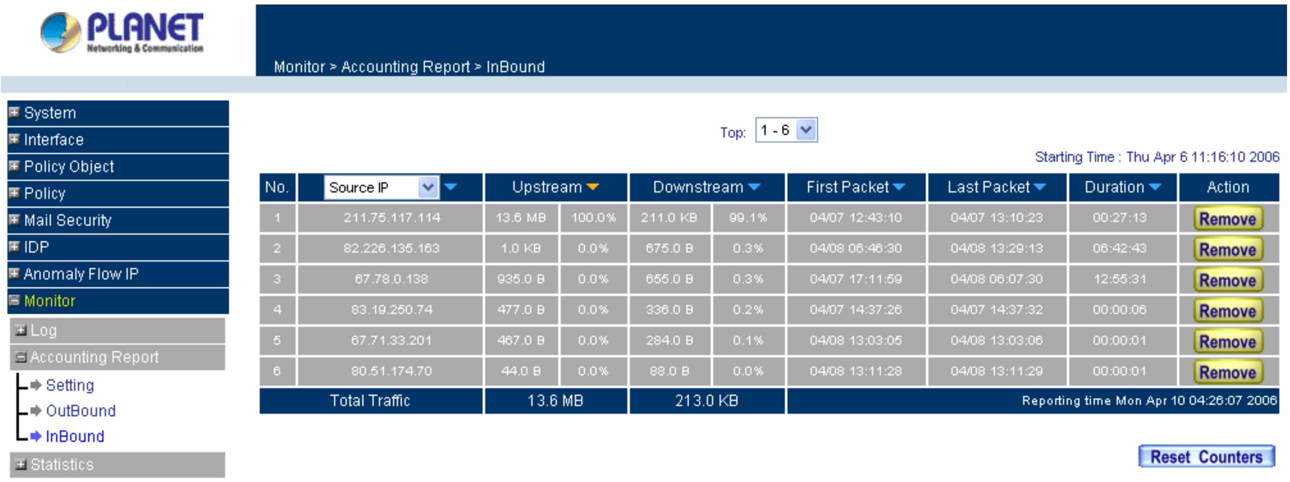
Top: 1 - 6

Starting Time : Thu Apr 6 11:16:10 2006

No.	Source IP	Upstream		Downstream		First Packet	Last Packet	Duration	Action
1	211.75.117.114	13.6 MB	100.0%	211.0 KB	99.1%	04/07 12:43:10	04/07 13:10:23	00:27:13	Remove
2	82.226.135.163	1.0 KB	0.0%	675.0 B	0.3%	04/08 06:46:30	04/08 13:29:13	06:42:43	Remove
3	67.78.0.138	935.0 B	0.0%	655.0 B	0.3%	04/07 17:11:59	04/08 06:07:30	12:55:31	Remove
4	83.19.250.74	477.0 B	0.0%	336.0 B	0.2%	04/07 14:37:26	04/07 14:37:32	00:00:06	Remove
5	67.71.33.201	467.0 B	0.0%	284.0 B	0.1%	04/08 13:03:05	04/08 13:03:06	00:00:01	Remove
6	80.51.174.70	44.0 B	0.0%	88.0 B	0.0%	04/08 13:11:28	04/08 13:11:29	00:00:01	Remove
Total Traffic		13.6 MB		213.0 KB		Reporting time Mon Apr 10 04:26:07 2006			

Inbound Source IP Accounting Report

Pull down the menu and select **Source IP** to show the inbound source IP accounting report.



Top: 1 - 6

Starting Time : Thu Apr 6 11:16:10 2006

No.	Source IP	Upstream		Downstream		First Packet	Last Packet	Duration	Action
1	211.75.117.114	13.6 MB	100.0%	211.0 KB	99.1%	04/07 12:43:10	04/07 13:10:23	00:27:13	Remove
2	82.226.135.163	1.0 KB	0.0%	675.0 B	0.3%	04/08 06:46:30	04/08 13:29:13	06:42:43	Remove
3	67.78.0.138	935.0 B	0.0%	655.0 B	0.3%	04/07 17:11:59	04/08 06:07:30	12:55:31	Remove
4	83.19.250.74	477.0 B	0.0%	336.0 B	0.2%	04/07 14:37:26	04/07 14:37:32	00:00:06	Remove
5	67.71.33.201	467.0 B	0.0%	284.0 B	0.1%	04/08 13:03:05	04/08 13:03:06	00:00:01	Remove
6	80.51.174.70	44.0 B	0.0%	88.0 B	0.0%	04/08 13:11:28	04/08 13:11:29	00:00:01	Remove
Total Traffic		13.6 MB		213.0 KB		Reporting time Mon Apr 10 04:26:07 2006			

When WAN users connect to LAN service server through CS-500, all of the Downstream / Upstream / First Packet / Last Packet / Duration log of the source IP will be recorded.

Definitions:

Top: Select the data type you want to check. It presents 10 results in one page.

Source IP: The IP address used by WAN host.

Downstream: The percentage of Downstream and the statistic value of the connection from LAN host to WAN host via CS-500.

Upstream: The percentage of Upstream and the statistic value of the connection from WAN host to LAN host via CS-500.

First Packet: The time record of the first packet that was sent from WAN host to LAN host.

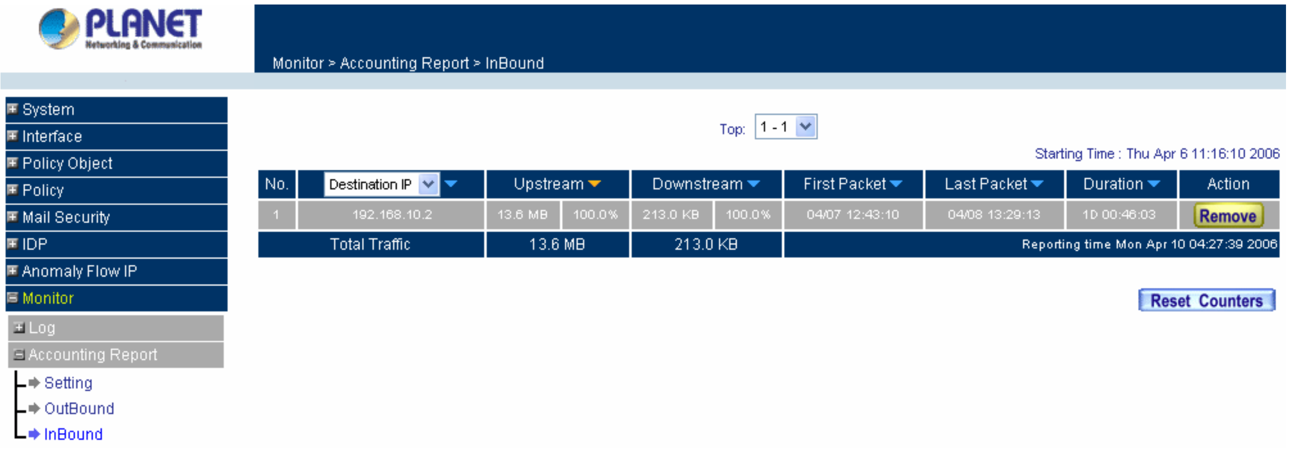
Last Packet: The time record of the last packet that sent from WAN host to LAN host.

Duration: The time statistic record that started from the first packet and end to the last packet.

Total Traffic: CS-500 will record the sum of upstream/downstream packets from WAN host to LAN host.

Inbound Destination IP Accounting Report

Pull down the menu and select **Destination IP** to show the inbound destination IP accounting report.



Monitor > Accounting Report > InBound

Top: 1 - 1

Starting Time : Thu Apr 6 11:16:10 2006

No.	Destination IP	Upstream		Downstream		First Packet	Last Packet	Duration	Action
1	192.168.10.2	13.6 MB	100.0%	213.0 KB	100.0%	04/07 12:43:10	04/08 13:29:13	1D 00:46:03	Remove
	Total Traffic	13.6 MB		213.0 KB		Reporting time Mon Apr 10 04:27:39 2006			

When WAN host connect to LAN through CS-500, all of the Downstream/Upstream/First Packet/Last Packet/Duration log of the Destination IP will be recorded.

Definitions:

Top: Select the data type you want to check. It presents 10 results in one page.

Destination IP: The IP address used by LAN host.

Downstream: The percentage of Downstream and the statistic value of the connection from WAN host to LAN host via CS-500.

Upstream: The percentage of Upstream and the statistic value of the connection from LAN host to WAN host via CS-500.

First Packet: The time record of the first packet that was sent from LAN host to WAN host.

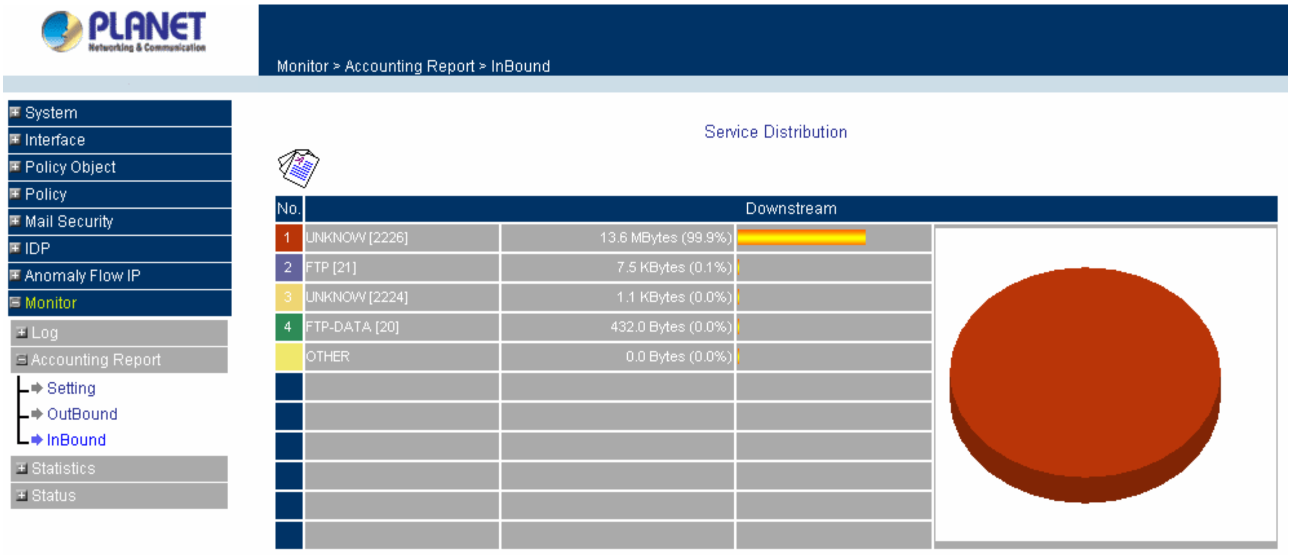
Last Packet: The time record of the last packet that sent from LAN host to WAN host.

Duration: The time statistic record that started from the first packet and end to the last packet.

Total Traffic: CS-500 will record the sum of upstream/downstream packets from LAN host to WAN host.

Inbound Service Accounting Report

Pull down the menu and select **Service** to show the inbound service accounting report.



Service Distribution

No.	Downstream		
1	UNKNOW [2226]	13.6 MBytes (99.9%)	
2	FTP [21]	7.5 KBytes (0.1%)	
3	UNKNOW [2224]	1.1 KBytes (0.0%)	
4	FTP-DATA [20]	432.0 Bytes (0.0%)	
	OTHER	0.0 Bytes (0.0%)	

When WAN host connect to LAN host through CS-500, all of the Downstream/Upstream/First Packet/Last Packet/Duration log of the Communication Service will be recorded.

Definitions:

Top: Select the data type you want to check. It presents 10 results in one page.

Service: The report of Communication Service when WAN host connect to LAN host through CS-500. **(Port)** indicates the protocol port number.

Downstream: The percentage of Downstream and the statistic value of the connection from WAN host to LAN host via CS-500.

Upstream: The percentage of Upstream and the statistic value of the connection from LAN host to WAN host via CS-500.

First Packet: The time record of the first packet that was sent to LAN host from WAN host.

Last Packet: The time record of the last packet sent to LAN host from WAN host.

Duration: The time statistic record that started from the first packet and end to the last packet

Total Traffic: CS-500 will record the sum of upstream/downstream packets from WAN host to LAN host.

NOTE: To correctly display the pizza chart, please install the latest java VM for http://www.java.com.

4.8.3 Statistic

In this chapter, the Administrator queries the Content Security Gateway for statistics of packets and data which passes across the Content Security Gateway. The statistics provides the Administrator with information about network traffics and network loads.

What is Statistics

Statistics are the statistics of packets that pass through the Content Security Gateway by control policies setup by the Administrator.

How to use Statistics

The Administrator can get the current network status from statistics, and use the information provided by statistics as a basis to mange networks.

How to apply WAN Statistics

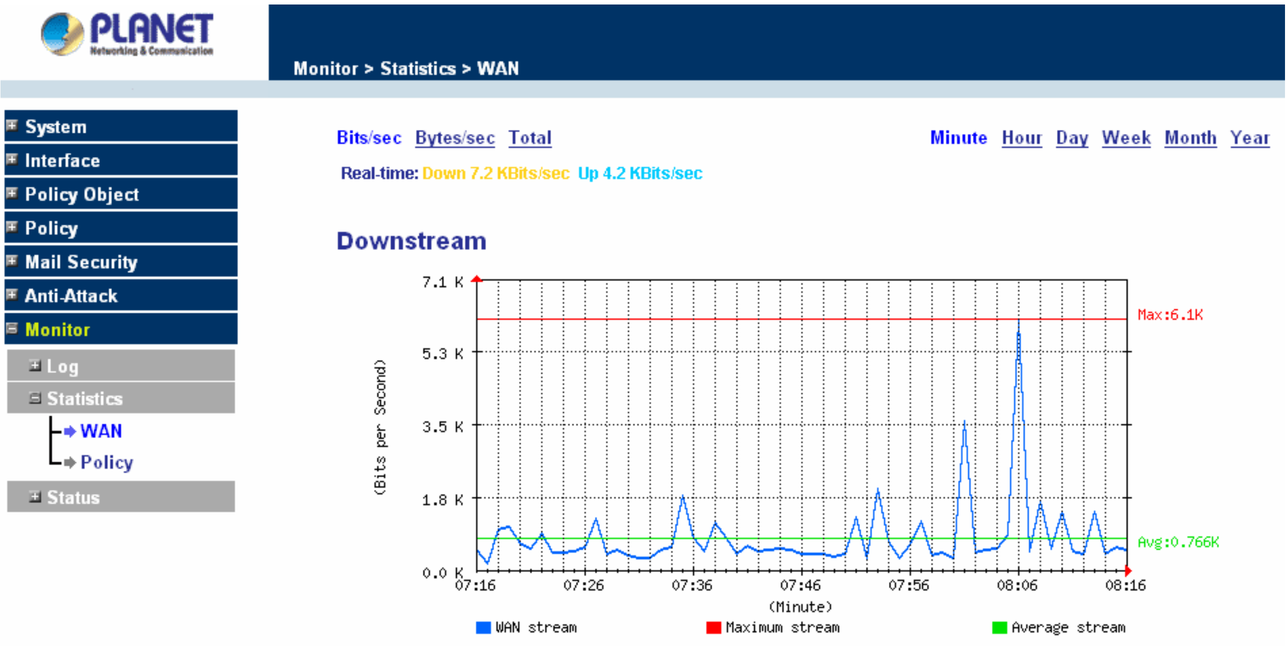
The Administrator needs to go to Policy to set the network IP addresses that you want to gather statistics. In this way, the administrator can handle the whole network condition and takes it as a basis of managing the network.

The administrator needs to go to the Policy to set the network IP of the statistics. By the WAN statistics you can obtain the status of the network.

4.8.3.1 WAN Statistics

Step 1. Click Statistics in the menu bar on the left hand side, and then select WAN Statistics.

Step 2. The WAN Statistics will be displayed. It displays statistics of WAN network connections (downstream and upstream as well) in a total amount by minute (60 minutes), hour (24 hours), day (30 days), Month and Year. Select the time units (minute, hour, day, month or year) of the graph.



Real-time: Down 7.2 KBits/sec Up 4.2 KBits/sec

Y-Coordinate: Four options are available: Total, Bits/sec, Bytes/sec and Utilization.

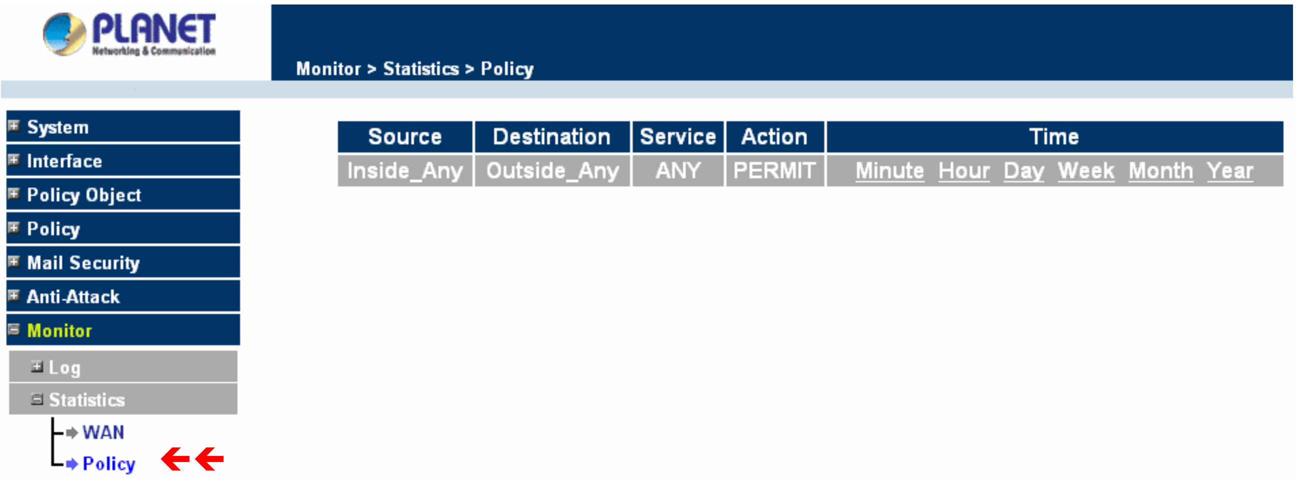
X-Coordinate: Time（Hour/Minute/Day）.

4.8.3.2 Policy Statistics

Entering the Statistics window

The Statistics window displays the statistics of current network connections.

- **Source:** the name of source address.
- **Destination:** the name of destination address.
- **Service:** the service requested.
- **Action:** permit or deny
- **Time:** viewable by minutes, hours, or days



Source	Destination	Service	Action	Time
Inside_Any	Outside_Any	ANY	PERMIT	Minute Hour Day Week Month Year

NOTE: To use Statistics, the administrator needs to go to Policy to enable Statistics function.

Entering the Policy Statistics

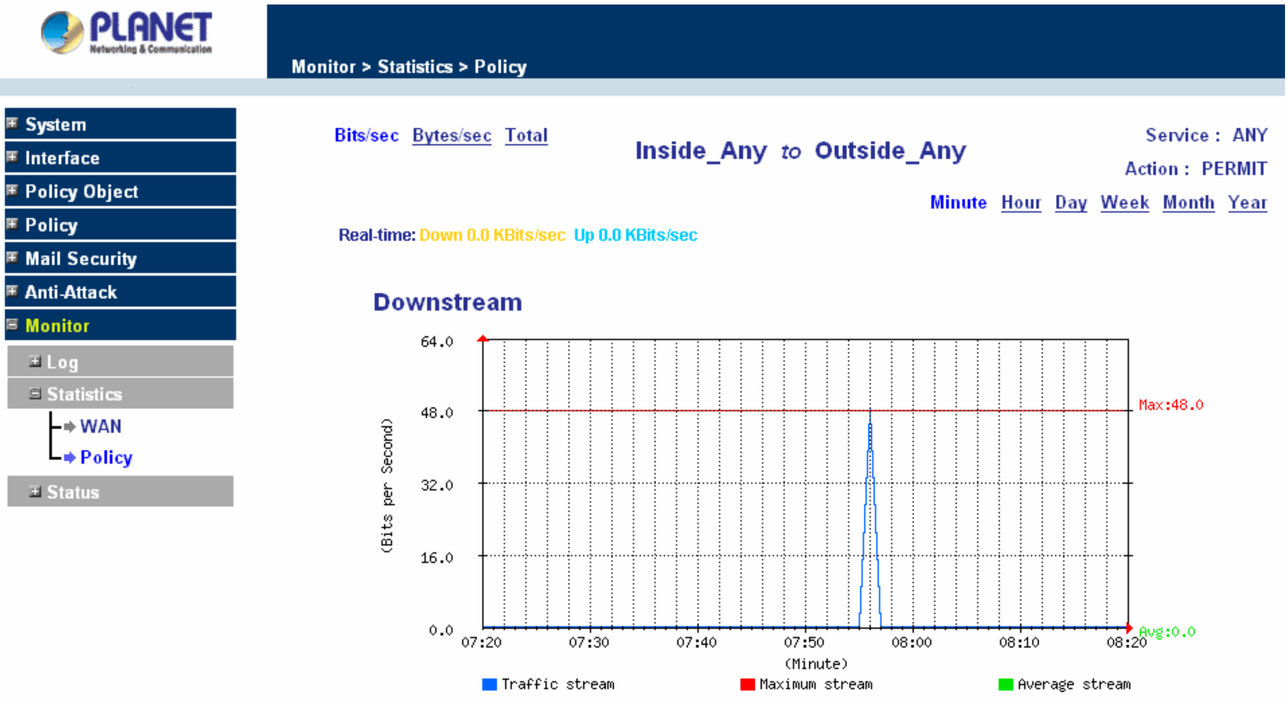
Step 1. Click **Statistics** in the menu bar on the left hand side, and then select **Policy Statistics**.

Step 2. In Statistics window, find the policy you want to view

Step 3. In the Statistics window, click Minute on the right hand side, and then you will be able to view the Statistics figure every minute; click Hour to view the Statistics figure every hour; click Day to view the Statistics figure every day.

Y-Coordinate: There are three options: Total, Kbit/sec, Kbytes/sec.

X-Coordinate: Time (Hour/Minute/Day).



Inside_Any to Outside_Any

Service : ANY

Action : PERMIT

Real-time: Down 0.0 KBits/sec Up 0.0 KBits/sec

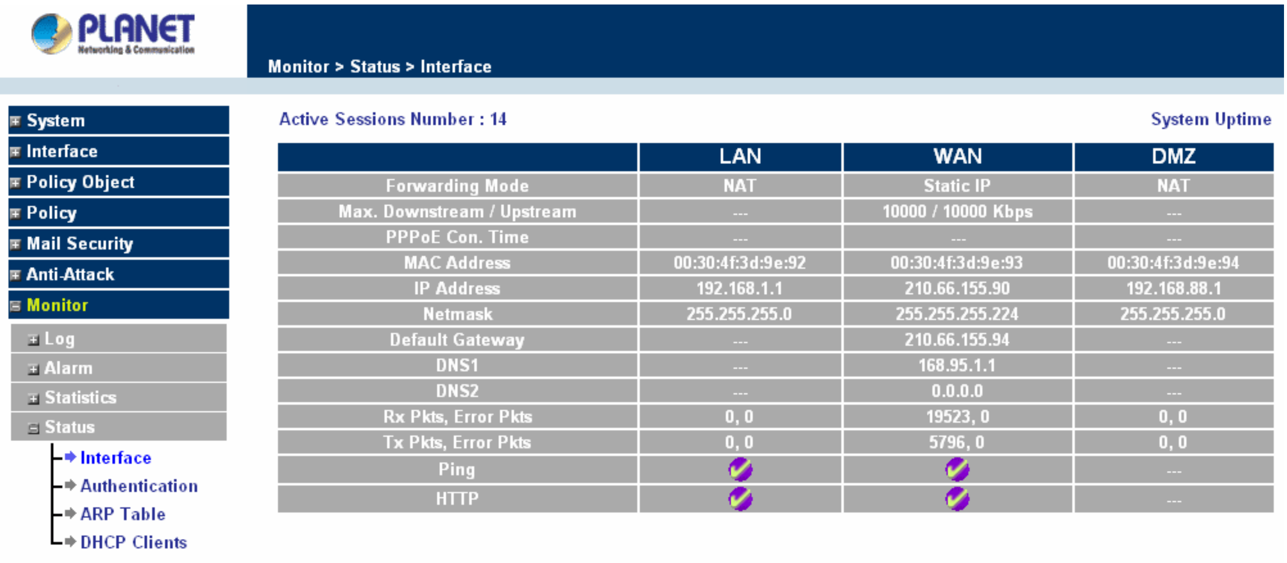
4.8.4 Status

In this section, the device displays the status information about the Content Security Gateway. Status will display the network information from the Configuration menu. The Administrator may also use Status to check the DHCP lease time and MAC addresses for computers connected to the Content Security Gateway.

4.8.4.1 Interface Status

Entering the Interface Status window

Click on **Status** in the menu bar, then click **Interface Status** below it. A window will appear providing information from the Configuration menu. **Interface Status** will list the settings for **LAN Interface**, **WAN Interface**, and the **DMZ Interface**.



Active Sessions Number : 14

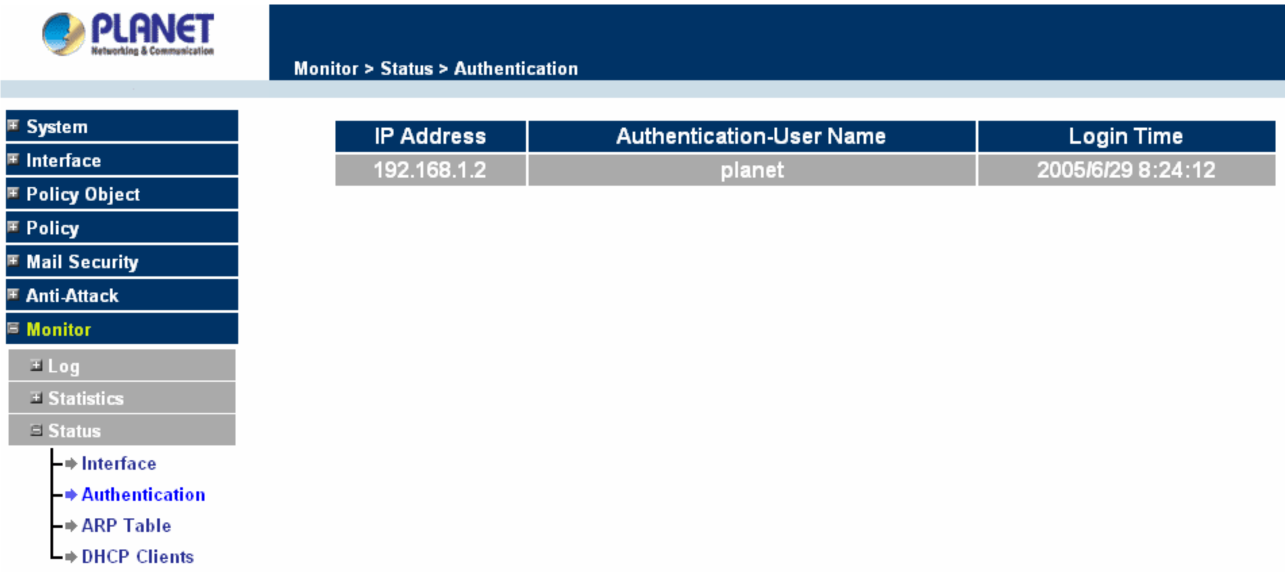
System Uptime

	LAN	WAN	DMZ
Forwarding Mode	NAT	Static IP	NAT
Max. Downstream / Upstream	---	10000 / 10000 Kbps	---
PPPoE Con. Time	---	---	---
MAC Address	00:30:4f:3d:9e:92	00:30:4f:3d:9e:93	00:30:4f:3d:9e:94
IP Address	192.168.1.1	210.66.155.90	192.168.88.1
Netmask	255.255.255.0	255.255.255.224	255.255.255.0
Default Gateway	---	210.66.155.94	---
DNS1	---	168.95.1.1	---
DNS2	---	0.0.0.0	---
Rx Pkts, Error Pkts	0, 0	19523, 0	0, 0
Tx Pkts, Error Pkts	0, 0	5796, 0	0, 0
Ping	✓	✓	---
HTTP	✓	✓	---

4.8.4.2 Authentication

Entering the Auth Status window

Click on **Status** in the menu bar, then click Authentication below it. A window will appear and provide information from the Auth User menu. Authentication Status will list the settings for Auth User login status.



IP Address	Authentication-User Name	Login Time
192.168.1.2	planet	2005/6/29 8:24:12

IP Address: The IP address of the host computer.

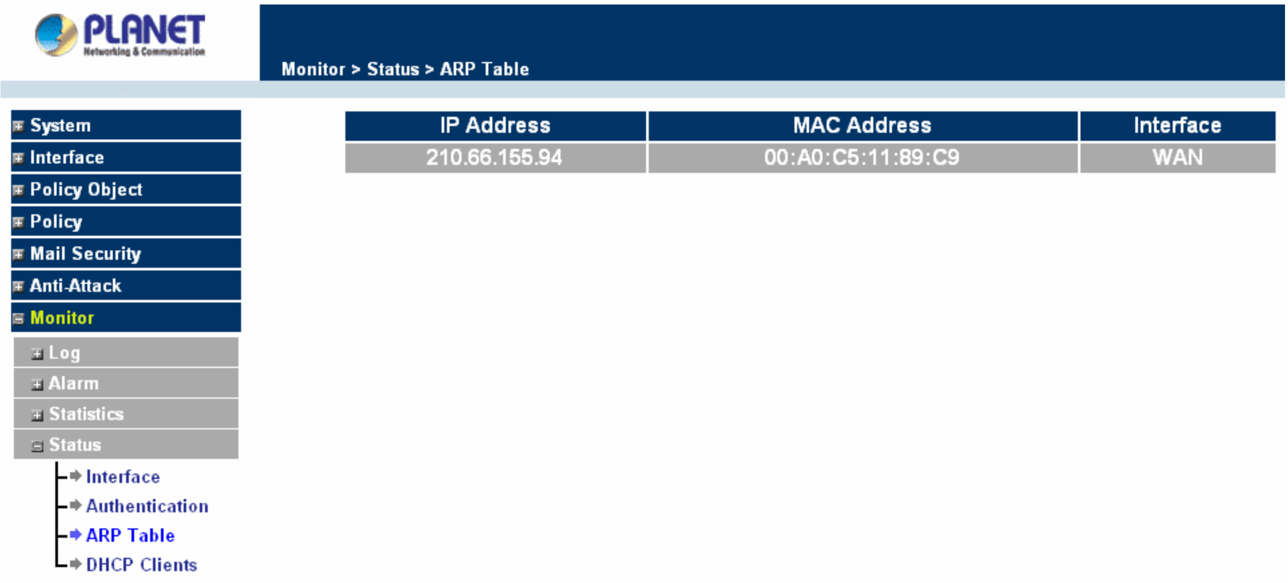
Auth-User Name: The Auth User Name of that host computer.

Login time: The Auth User login in time.

4.8.4.3 ARP Table

Entering the ARP Table window

Click on **Status** in the menu bar, then click **ARP Table** below it. A window will appear displaying a table with IP addresses and their corresponding MAC addresses. For each computer on the LAN, WAN, and DMZ network that replies to an ARP packet, the device will list them in this ARP table.



IP Address	MAC Address	Interface
210.66.155.94	00:A0:C5:11:89:C9	WAN

IP Address: The IP address of the host computer

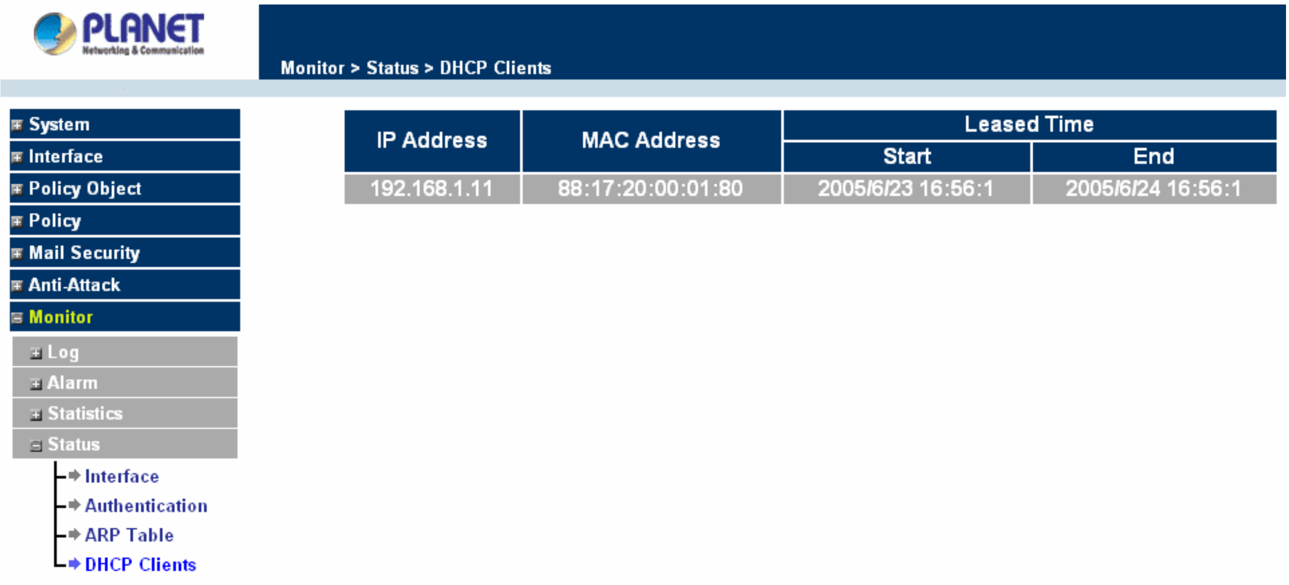
MAC Address: The MAC address of that host computer

Interface: The port that the host computer is connected to (LAN, WAN, DMZ)

4.8.4.4 DHCP Clients

Entering the DHCP Clients window

Click on **Status** in the menu bar, then click on **DHCP Clients** below it. A window will appear displaying the table of DHCP clients that are connected to the device. The table will list host computers on the LAN network that obtain its IP address from the Content Security Gateway’s DHCP server function.



IP Address	MAC Address	Leased Time	
		Start	End
192.168.1.11	88:17:20:00:01:80	2005/6/23 16:56:1	2005/6/24 16:56:1

IP Address: the IP address of the LAN host computer

MAC Address: MAC address of the LAN host computer

Leased Time: The Start and End time of the DHCP lease for the LAN host computer.